No One Behind

Træningsmanual for en digital kompetent borger

Co-funded by the Erasmus+ Programme

Dette projekt er blevet finansieret med støtte fra Europa-Kommissionen. Denne publikation afspejler kun forfatterens synspunkter, og Kommissionen kan ikke holdes ansvarlig for enhver brug, der kan gøres af

No One Behind

Co-funded by the Erasmus+ Programme of the European Union

Uddannelsesmanual for en "digital kompetent" borger

Erasmus Plus Program – KA2 Strategisk Partnerskab for Voksenuddannelse

Bestående af:

P1 – Agentia Nationala pentru Programe Comunitarie i Domiul Educariei si Formarii Profesionale - NERDA - RO
P2 - EUROCREA MERCHANT SRL – EUROCREA - IT
P3 - INOVA+ - INNOVATIONSSERVICES, SA – INOVA+ - PT
P4 - Asociatia de Dezvoltare Locala ECO LAND - ADL "ECO LAND" - RO
P5 - AINTEK SYMVOULOI EPICHEIRISEON EFARMOGES YPSILIS TECHNOLOGIAS EKPAIDEFSY ANONYMI ETAIREIA IDEC – GR
P6 - European E-Learning Institute - EUEI – DK
P7 - ATERMON BV – ATERMON - NL

FORFATTER | Ingen bagved | august 2021

Partnerskab

North-East Regional Development Agency - NERDA, Rumænien
Lucian Alexa og Olivian Secara
Hjemmeside: https://www.adrnordest.ro/en/homepage/

Eurocrea Merchant, SRL, Italien
Beatrice Del Nero
Hjemmeside: http://www.eurocreamerchant.it/

INOVA+ - Innovation Services SA, Portugal
Andreia Monteiro og Sara Correia
Hjemmeside: https://inova.business/

ØKOLAND, Rumænien
Ciprian Barsan
Facebook: https://www.facebook.com/AdlEcoLand/

IDEC, Grækenland
Rafaela Paspati og Lila Anthopoulou
Hjemmeside: https://idec.gr/

European E-Learning Institute – EUEI, Danmark
Canice Hamill og Catherine Neill
Hjemmeside: https://www.euei.dk/

ATERMON, Holland
Anna Stamouli
Hjemmeside: https://www.atermon.nl/

INDHOLDSFORTEGNELSE

RESUMÉ 9

INTRODUKTION 11

1. Introduktion til No One Behind træningsmanualen 9
2. Profil på den "digitalt kompetente" borger 11

DIGITAL KOMPETENT BORGERLÆSNING 13

1. Modul 1: Information og datafærdighed 18
   - **1.1. Gennemse, søge og filtrere data** 20
   - **1.1.1. Hovedbegreber: IT, IKT og internet** 21
   - **1.1.2. Introduktion til søgning på nettet** 22
   - **1.1.3. Beskyttelse ved brug af IKT** 24
   - **1.1.4. Praktiske aktiviteter** 26
   - **1.2. Evaluering af data, information og digitalt indhold** 31
   - **1.2.1. Hvordan vurderer man kilder og information online?** 31
   - **1.2.2. Evaluering af dine kilder** 33
   - **1.2.3. Evaluering af hjemmesider** 33
   - **1.2.4. Fakta-tjek hjemmesider** 35
   - **1.2.5. Praktiske aktiviteter** 35
   - **1.3. Håndtering af data, information og digitalt indhold** 39
   - **1.3.1. Enheder til at gemme og hente oplysninger** 39
   - **1.3.2. Ophavsret og databeskyttelse** 42
   - **1.3.3. Praktiske aktiviteter** 44
2. Modul 2: Kommunikation og samarbejde og samarbejde 47
   - **2.1. Interagere gennem digitale teknologier** 49
   - **2.2. Deling gennem digitale teknologier** 56
   - **2.3. Engagere sig i medborgerskab gennem digitale teknologier** 61
   - **2.4. Samarbejde gennem digitale teknologier** 69
   - **2.5. Netiquette** 75
   - **2.6. Håndtering af digital identitet** 82
3. Modul 3: Indholdsskabelse 87
   - **3.1. Udvikling af digitalt indhold** 88
   - **3.2. Integrering og re-udarbejdelse af digitalt indhold** 91

3.3. Copyright og licenser 94

3.4. Programmering 96

4. Modul 4: Sikkerhed 101

4.1. Beskyttelse af enheder 102

4.1.1. Beskyttelse af enheder 102

4.1.2. Softwareopdateringer 106

4.1.3. Sikkerhed og adgangskoder 108

4.1.4. Øget sikkerhed 112

4.1.5. Hvad er ondsindet kode? 120

4.1.6. Praktiske aktiviteter 124

4.2. Beskyttelse af personlige data og privatliv 128

4.2.1. Beskyt dig selv online 128

4.2.2. Retningslinjer for deling af personlige oplysninger 131

4.2.3. Praktiske aktiviteter 134

4.3. Beskyttelse af sundhed og velvære 137

4.3.1. Negative virkninger af teknologi: hvad man skal vide 137

4.3.2. Har du hørt om cybermobning? 142

4.3.3. Praktiske aktiviteter 144

4.4. Beskyttelse af miljøet 146

4.4.1. Korrekt bortskaffelse af elektroniske enheder 147

4.4.2. Praktiske aktiviteter 150

5. Modul 5: Problemløsning 153

5.1. Løsning af tekniske problemer 154

5.1.1. Computere og dets systemer 154

5.1.2. De mest almindelige tekniske problemer ..... **Error! Bookmark not defined.**

5.1.3. Praktiske aktiviteter 160

5.2. Identificering af behov og teknologiske reaktioner 162

5.2.1. Identificering af behov og teknologiske reaktioner 162

5.2.2 Praktiske aktiviteter 167

5.3. Kreativ brug af digitale teknologier 177

5.4. Identificering af digitale kompetencegab 183

EVALUERING AF UDDANNELSEN 189

1. Evaluering af læringen 190
2. Evaluering af uddannelsen 193
BILAG 194
Bilag I – Yderligere ressourcer 195
Bilag II – Evalueringsark Modul 1. Information og datafærdighed 200
Bilag III – Evalueringsark Modul 2 201
Bilag IV – Evalueringsark Modul 3 203
Bilag IV – Evalueringsark Modul 4 204
Bilag V – Evalueringsark Modul 5 205
Bilag VI – Evaluering af uddannelsen 206
REFERENCER 208

TABEL MED FIGUR

Figur 1 – Oversigt og global struktur for Digital Competent Citizen-profilen, som defineret af konsortiet og i overensstemmelse med ECVET 11
Figur 2 – Identifikation af de kompetenceenheder, der svarer til modulerne i profilen for en digital kompetent borger. 12
Figur 3 – Ikoner for nogle browsere. 22
Figur 4 – Googles hjemmeside. 23
Figur 5 – Chrome-hjemmeside. 23
Figur 6 – Identifikation af låseikonet. 25
Figur 8 – identifikation og kort beskrivelse af hukommelse og lagerenheder. 41
Figur 9 – Retningslinjer vedrørende beskyttelse af personoplysninger som fastsat i direktiv 95/46/EF. 44
Figur 10 – Identifikation af mulige situationer, der skal tages i betragtning i denne aktivitet. 44
Figur 11 – Inddeling af elever i to grupper. 45
Figur 12 – Profiler, der skal overvejes for at forberede adgangskoder. 86
Figur 13 – Data til beregning af strømforbruget. 151

TABEL OVER TABELLER

Tabel 1 – Studieordning for uddannelsesforløbet Digital Competent Citizen. 14
Tabel 2 – Kort beskrivelse og identifikation af kompetenceenhederne for hvert modul i uddannelsesforløbet. 16
Tabel 3 – Identifikation og kort beskrivelse af de metoder, der tages i betragtning i denne manual. ..... **Error! Bookmark not defined.**
Tabel 4 – Global struktur af modul 1 – Information og datafærdighed. 19
Tabel 5 – Kompetenceenhedens opbygning 1.1. - Gennemse, søge og filtrere data fra Modul 1 – Information og datafærdighed. 20

Tabel 6 - Kompetenceenhedens opbygning 1.2. Evaluering af data, information og digitalt indhold i Modul 1 – Information og datafærdighed 31
Tabel 7 – Liste over bekræftelser og korrekt svar. 36
Tabel 8 - Kompetenceenhedens opbygning 1.3. Håndtering af data, information og digitalt indhold i Modul 1 – Information og datafærdighed. 39
Tabel 9 - Global struktur af modul 2 - Kommunikation og samarbejde. 48
Tabel 10 - Kompetenceenhedens opbygning 2.1. – Interagere gennem digitale teknologier i Modul 2 – Kommunikation og samarbejde. 49
Tabel 11 - Kompetenceenhedens opbygning 2.2. – Deling gennem digitale teknologier af Modul 2 – Kommunikation og samarbejde. 56
Tabel 12 - Kompetenceenhedens opbygning 2.2. – Engagere sig i medborgerskab gennem digitale teknologier i modul 2 – Kommunikation og samarbejde. 61
Tabel 13 - Kompetenceenhedens opbygning 2.5. – Samarbejde gennem digitale teknologier i Modul 2 – Kommunikation og samarbejde. 69
Tabel 14 - Kompetenceenhedens opbygning 2.6. – Netiquete for Modul 2 – Kommunikation og samarbejde. 75
Tabel 15 - Kompetenceenhedens opbygning 2.7. – Håndtering af digital identitet af Modul 2 – Kommunikation og samarbejde. 82
Tabel 16 - Global struktur af modul 3 - Oprettelse af indhold. 88
Tabel 17 - Kompetenceenhedens opbygning 3.1.- Udvikling af digitalt indhold i Modul 3 – Indholdsskabelse. 88
Tabel 18 Kompetenceenhedens opbygning 3.2. – Integrering og re-udarbejdelse af digitalt indhold i Modul 3 – Indholdsskabelse. 91
Tabel 19 - Kompetenceenhedens opbygning 3.3.- Ophavsret og licenser til Modul 3 – Indholdsoprettelse. 94
Tabel 20 - Kompetenceenhedens opbygning 3.4. - Programmering af modul 3 – Indholdsskabelse. 96
Tabel 21 - Global struktur af modul 4 - Sikkerhed. 101
Tabel 22 - Kompetenceenhedens opbygning 4.1. – Beskyttelsesanordninger i modul 4 – Sikkerhed. 102
Tabel 23 - Kompetenceenhedens opbygning 4.2. – Beskyttelse af personlige data og privatlivets fred for Modul 4 – Sikkerhed. 128
Tabel 24 - Kompetenceenhedens opbygning 4.3. – Beskyttelse af sundhed og velvære i Modul 4 – Sikkerhed. 137
Tabel 25 - Kompetenceenhedens opbygning 4.4. – Beskyttelse af miljøet i Modul 4 – Sikkerhed. 147
Tabel 26 - Global struktur af modul 5 - Problemløsning. 153
Tabel 27 - Kompetenceenhedens opbygning 5.1. – Løsning af tekniske problemer i modul 5 – Problemløsning. 154
Tabel 28 - Kompetenceenhedens opbygning 5.2. – Identificering af behov og teknologiske reaktioner i modul 5 – Problemløsning. 162
Tabel 29 - Kompetenceenhedens opbygning 5.3. – Kreativ brug af digitale teknologier fra Modul 5 – Problemløsning. 177
Tabel 30 - Kompetenceenhedens opbygning 5.4. – Identifikation af mangler i digitale kompetencer i Modul 5 – Problemløsning 183
Tabel 31 – Identifikation af beviskriterierne for hver kompetenceenhed til vurdering af kompetencedomænet af voksne elever. 192

FORKORTELSER

EQF	European Qualification Framework
ECVET	Europæisk meritsystem for erhvervsuddannelse

No One Behind

Co-funded by the Erasmus+ Programme of the European Union

RESUMÉ

Uddannelsesmanualen for en digital kompetent borger er udviklet inden for rammerne af ***Ingen bagved*** projekt, der skal guide undervisere og elever gennem en nem vej til at fremme digitale færdigheder hos voksne fra landdistrikter.

Manualen indeholder en uddannelsesplan og materialer til at støtte voksenundervisere (og andre interessenter) i udviklingen af digitale færdigheder hos voksne fra landdistrikterne, hvilket giver dem mulighed for at blive "digitalt kompetente borgere".

Uddannelsespensum var struktureret ud fra profilen af **digital kompetent borger**, også designet af konsortiet i overensstemmelse med principperne for det europæiske meritsystem for erhvervsuddannelse (ECVET)[1] og den europæiske kvalifikationsramme (EQF)[2]. Profilen præsenteres kort i begyndelsen af denne manual.

Med hensyn til struktur og indhold hænger pensum og materialer sammen medDigComp – European Digital Competence Framework for borgere og indeholder således 5 træningsmoduler, der dækker rammens 21 digitale kompetencer:

- Information og datafærdighed
- Kommunikation og samarbejde
- Oprettelse af digitalt indhold
- Sikkerhed
- Problemløsning

For hvert af disse moduler giver denne manual:

- et overblik over de mål, indhold og struktur, der skal følges af voksenundervisere og elever;
- specifikke planer, aktiviteter og ressourcer relateret til de kompetenceenheder, der er identificeret i hvert modul, og som fremmer udviklingen og styrkelsen af voksnes digitale færdigheder.

Er også en del af dette dokument et sæt gitter til at understøtte vurderingen af udviklingsniveauet for digitale kompetencer hos voksne fra landdistrikterne, der skal udføres før og efter træningen finder sted.

[1] European Qualification Framework: flere oplysninger om dette kan findes her.
[2] Europæisk meritsystem for erhvervsuddannelse: flere oplysninger om dette kan findes her.

No One Behind

Co-funded by the Erasmus+ Programme of the European Union

INTRODUKTION

1. Introduktion til No One Behind træningsmanualen

Denne træningsmanual er resultatet af det fælles arbejde af forskellige organisationer, der tænker på at producere en trin-for-trin guide til at fremme digitale færdigheder hos grupper af mennesker, der bor i landdistrikter, og fremme social inklusion ved at øge deres digitale kompetencer. Enhederne og indholdet er organiseret på en måde, så manualen kan bruges til selvlæring, men også som et værktøj/vejledning for undervisere, der ønsker at give en undervisning om digitale færdigheder til mennesker, der har meget få digitale kompetencer.

Hvem er denne manual til?

Voksenundervisere: socialrådgivere, lærere, mentorer, professorer og andre fagpersoner, der arbejder med voksne;

Voksne fra landdistrikter, der er villige til at forbedre deres dagligdag, at skifte job eller finde nye muligheder ved at udvikle nyttige digitale færdigheder.

Formålet med denne manual er at guide undervisere og elever gennem en nem og innovativ vej til at fremme digitale færdigheder, efter retningslinjerne i DigComp-rammen.

Manualen er organiseret i fire hovedafsnit som følger:

- **Executive Summary** – Med en syntese af indholdet af træningsmanualen, der kan bruges til at introducere den til målgrupper og sociale medier.
- **Introduktion** – Startende med en kort introduktion til træningsmanualen og med en kort oversigt over profilen for den "digitalt kompetente" borger præsenteret i metoden[3].
- **Digital kompetent borgerpensum**– Den består af fem kapitler svarende til uddannelsens fem moduler. Hvert kapitel giver information om modulets struktur og de tilsvarende kompetenceenheder. Det giver også retningslinjer og materialer til at understøtte implementeringen af træningen og erhvervelsen/forstærkningen af elevernes digitale kompetencer.
- **Evaluering af uddannelsen**– Denne sektion giver retningslinjer i forbindelse med evaluering af elevers digitale kompetencer og læring og giver støtte til at sikre det. Det giver også støtte til elevernes evaluering af træningen.

Et sæt bilag til støtte for implementeringen af uddannelsen findes også i dette dokument, herunder:

- Bilag I – Yderligere ressourcer – Med links relateret til moduler og kompetenceenheder inkluderet i denne træningsmanual, som undervisere og elever kan få adgang til at vide mere.
- Bilag II – Evalueringsark Modul 1 – Et evalueringsskema, der skal bruges til at måle udviklingsniveauet for elevernes digitale kompetencer relateret til information og datafærdighed.

[3]Den fulde præsentation af profilen er tilgængelig i dokumentet Innovativ metode til at uddanne og træne voksne fra landdistrikterne til at forbedre deres digitale og ikt-færdigheder. Tilgængelighed.

- Bilag III – Evalueringsark Modul 2 – Et evalueringsskema, der skal bruges til at måle udviklingsniveauet for elevernes digitale kompetencer relateret til kommunikation og samarbejde.
- Bilag IV – Evalueringsark Modul 3– Et evalueringsskema, der skal bruges til at måle udviklingsniveauet for elevernes digitale kompetencer relateret til indholdsskabelse.
- Bilag IV – Evalueringsark Modul 4– Et evalueringsskema, der skal bruges til at måle udviklingsniveauet for elevernes digitale kompetencer relateret til sikkerhed.
- Bilag V – Evalueringsark Modul 5– Et evalueringsskema, der skal bruges til at måle udviklingsniveauet for elevernes digitale kompetencer relateret til problemløsning.
- Bilag VI – Evaluering af uddannelsen - Evalueringsskema til elevernes evaluering af kvaliteten og relevansen af uddannelsen.

2. Profil på den "digitalt kompetente" borger

Bag det kursus, der introduceres i denne manual, er profilen for den "digitale kompetente" borger, defineret som vist i skemaet nedenfor (Figur 1.):

Digital kompetent borger

OVERSIGT

EQF[4] Niveau

3

EQF-kreditter: 5

Beskrivelse: Den "digitale kompetente" borger vil være i stand til at:

- forstå nytten af digitale kompetencer
- bruge de vigtigste digitale systemer i hverdagen
- forstå risici og mulige trusler forbundet med internetmiljøet
- forstå, hvordan man interagerer med andre og bruger teknologier til at få adgang til tjenester

GLOBAL STRUKTUR

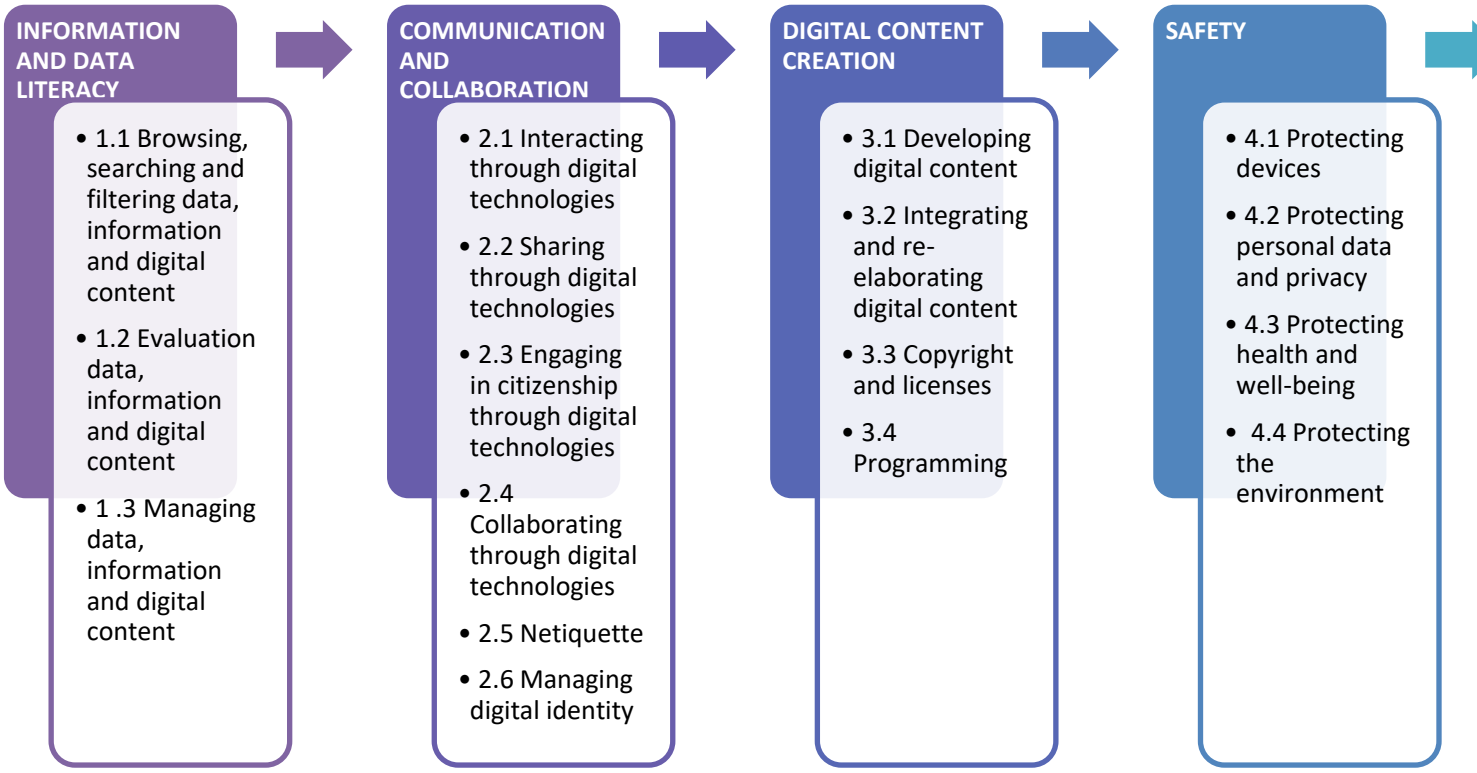
Nr.	modul	Varighed	Kredit
1	Information og datafærdighed	25 timer	1
2	Kommunikation og samarbejde	25 timer	1
3	Digitalt indholdsskabelse	25 timer	1
4	Sikkerhed	25 timer	1
5	Problemløsning	25 timer	1

Figur 1 – Oversigt og global struktur for Digital Competent Citizen-profilen, som defineret af konsortiet og i overensstemmelse med ECVET[5].

Hvert modul er struktureret i kompetenceenheder, som er afgørende for at vejlede voksenundervisere og elever i tilegnelsen, udviklingen og konsolideringen af digitale kompetencer (figur 2).

[4] European Qualification Framework: flere oplysninger om dette kan findes her.

[5] Europæisk meritsystem for erhvervsuddannelse: flere oplysninger om dette kan findes her.



Figur 2 – Identifikation af de kompetenceenheder, der svarer til modulerne i profilen for en digital kompetent borger.

Disse kompetenceenheder er beskrevet i dokumentet Innovativ metode til at uddanne og træne voksne fra landdistrikterne for at forbedre deres digitale og ikt-færdigheder[6] i form af viden, færdigheder og kompetencer

[6] Tilgængelig her.

No One Behind

Co-funded by the Erasmus+ Programme of the European Union

DIGITAL KOMPETENT BORGER

LÆREPLAN

Dette afsnit er dedikeret til **Digital kompetent borger** læseplan, hvor du har adgang til:

- et globalt overblik over læreplanens opbygning;
- kort præsentation af de 5 moduler, der udgør læseplanen;
- specifikke planer, aktiviteter og ressourcer relateret til de kompetenceenheder, der er identificeret i hvert modul, og som fremmer udviklingen og styrkelsen af voksnes digitale færdigheder.

Tabel 1. Præsenterer den globale struktur af **Digital kompetent borger** læseplan som struktureret i omfanget af No One Behind-projektet:

Træningsbane	**Digital kompetent borger**
Varighed	125 timer
Mål	Kombination af face-to-face session med online sessioner og selvstudie.
Træningsorganisation	Blandet læring, der kombinerer træning ansigt til ansigt med online sessioner.
Hovedmål	Denne manual har til formål at blive en reference for undervisere, når de arbejder med voksne med lave digitale færdigheder. For at nå dette mål omfatter manualen teoretisk indhold og praktiske aktiviteter for at fremkalde læring. Denne manual har til formål at støtte praktikanter og voksne med at forbedre deres digitale færdigheder ved at tilbyde trinvise aktiviteter.
Træningsplan	Kurset er opbygget i fem moduler: • Modul 1 - Information og datafærdighed (25 timer) • Modul 2 - Kommunikation og samarbejde (25 timer) • Modul 3 - Digitalt indholdsskabelse (25 timer) • Modul 4 – Sikkerhed (25 timer) • Modul 5 - Problemløsning (25 timer)
Læringsvurdering	Vurderingsark for hvert modul og hver enhed (leveres i slutningen af manualen)
Træningsvurdering	Vurderingsark (leveres i slutningen af manualen)

Bord 1 – Curriculum for uddannelsesforløbet Digital Competent Citizen.

Som det kan ses, er læseplanen organiseret i 5 moduler, hver med et specifikt forslag og opdelt i kompetenceenheder som vist i tabel 2.:

Modul 1 **Information og datafærdighed**	
Dette modul introducerer de værktøjer og kompetencer, der er nødvendige for at udføre onlinesøgning, samtidig med at der præsenteres forskellige strategier og teknikker til at finde pålidelig information. Ved afslutningen af dette modul forventes det, at eleverne ved, hvordan man håndterer information, er i stand til at gemme den i teknologiske enheder, genfinde den, selvom de er opmærksomme på love om ophavsret og databeskyttelse.	1.1. Gennemse, søge og filtrere data
	1.2. Evaluering af data, information og digitalt indhold
	1.3. Håndtering af data, information og digitalt indhold
Modul 2 **Kommunikation og samarbejde**	
I dette modul vil eleverne udvikle færdigheder og evner til at engagere sig med andre ved hjælp af digital teknologi. De vil være i stand til at interagere og dele informationer, idet de er opmærksomme på netiquette og personlig identitet online.	2.1. Interagere gennem digitale teknologier
	2.2. Deling gennem digitale teknologier
	2.3. Engagere sig i medborgerskab gennem digitale teknologier
	2.4. Samarbejde gennem digitale teknologier
	2.5. Netiquette
	2.6. Håndtering af digital identitet
Modul 3 **Digitalt indholdsskabelse**	
Målet med dette modul er at fremme kompetencer til at skabe digitalt indhold og programmering, så eleverne føler sig trygge ved for eksempel at promovere deres egen virksomhed online.	3.1. Udvikling af digitalt indhold
	3.2. Integrering og re-udarbejdelse af digitalt indhold
	3.3. Copyright og licenser
	3.4. Programmering
Modul 4 **Sikkerhed**	
Når de gennemfører dette modul, skal eleverne blive opmærksomme på de handlinger, de kan tage for at beskytte enheder, deres sundhed og miljøet, når de bruger teknologi. Dette modul har også til formål at øge bevidstheden om privatliv og personlige data.	4.1. Beskyttelse af enheder
	4.2. Beskyttelse af personlige data og privatliv
	4.3. Beskyttelse af sundhed og velvære
	4.4. Beskyttelse af miljøet
Modul 5 **Problemløsning**	
Dette modul fremhæver tekniske problemer og strategier til at håndtere de mest aktuelle problemer, når du betjener en	5.1. Løsning af tekniske problemer
	5.2. Identificering af behov og teknologiske reaktioner

computer. Derudover vil eleverne have mulighed for at tænke på kreative metoder, når de bruger digitale værktøjer.	5.3. Kreativ brug af digitale teknologier
	5.4. Identificering af digitale kompetencegab

Bord 2 – Kort beskrivelse og identifikation af kompetenceenhederne for hvert modul i uddannelsesforløbet.

Efter denne struktur kan du i dette afsnit finde fem kapitler, som hver svarer til et af modulerne i læseplanen. I begyndelsen af hvert kapitel vil du have en tabel med en oversigt over varigheden, målene og enheder, der er dækket i modulet. Den følger præsentationen for kompetenceenhederne med hensyn til varighed, mål, indhold, ressourcer og træningsmetoder og hvordan enhederne kunne leveres. Til hver enhed finder du både teoretisk information og praktiske aktiviteter, så læringsoplevelsen flyder let og forhåbentlig muliggør en "hands-on" tilgang.

Derfor foreslås mange aktiviteter gennem hele manualen, der gør brug af forskellige læringsmetoder såsom:

Metode	Beskrivelse
Præsentation af træner	Elevernes deltagelse i lektioner baseret på PowerPoint-præsentationer, videovisualisering, demonstration, forskningsstudier, bøger, artikler eller andre ressourcer og støtte, der vises af underviserne i en træningssession eller e-læringsplatform. Yderligere support - casestudier, opgaver og quizzer - kan bruges, hvilket muliggør konsolidering af deres ekspertise og øget viden.
Gruppeøvelse Diskussion / Debat	Det kan laves i store eller mindre grupper, og ideen er at fremme diskussionen eller debatten mellem elever relateret til et specifikt emne, som underviseren har lanceret. Diskussionen eller debatten bør overvåges for at tillade deltagelse af alle elever og fokus på de relevante emner. I slutningen af diskussionen eller debatten er det vigtigt at udarbejde og dele nogle konklusioner.
Arbejde i par/små grupper	Underviseren skal give hver lille gruppe nøjagtige oplysninger om emnet, de forventede resultater af gruppearbejdet (også metoden til præsentation af resultaterne – gruppen skal være klar over, hvem der skal præsentere disse resultater i begyndelsen af arbejdet) og varigheden af gruppearbejdet. Inden øvelsen påbegyndes, tjekker træneren og alle eleverne tiden, og træneren fortæller eleverne, hvornår de skal mødes igen i den store gruppe for at undgå eventuelle misforståelser. Under gruppearbejdet assisterer træneren alle grupper og holder øje med tidsplanen.
Præsentation af deltagere	Undervisere kan udfordre eleverne til at forberede en præsentation om et bestemt emne og moderere en læringssession. Eleverne kan vælge præsentationsformatet (f.eks. PowerPoints, aktiviteter, videoer,...) og engagere andre elever i præsentationens forskellige øjeblikke.
Simulering / Rollespil	Rollespil er en læringsmetode, hvor eleverne påtager sig roller som karakterer og i fællesskab skaber historier. Denne teknik er et glimrende værktøj til at engagere eleverne og give dem mulighed for at interagere med deres jævnaldrende, mens de forsøger at fuldføre den opgave, de har fået tildelt i deres specifikke rolle. Dette arbejde kan udføres i samarbejdsgrupper, og/eller eleverne kan bevare deres rolles persona gennem hele klasseperioden. Eleverne er mere engagerede, når de forsøger at reagere på materialet fra deres karakters perspektiv.
Projektbaseret læring (PBL)	PBL er en undervisning baseret på projekter eller integrerede opgaver. Med udgangspunkt i et konkret problem bliver eleverne udfordret til at udvikle projekter, der reagerer på problemer i det virkelige liv, hvilket giver dem mulighed for aktivt at blive involveret i deres læring, lære ved at gøre og erhverve/forstærke deres færdigheder.

Kooperativ læring	Det er en diskussionsbaseret metode, hvor en lille gruppe elever diskuterer et emne, der er lanceret af underviseren. Tre hovedroller skal fordeles blandt eleverne:) skribenten tager notater til debatten, så alle de andre elever kan være fuldt ud involveret i samtalen; 2) den lille kortskuffe overvåger, hvem der taler og hvornår og tegner samtalens udvikling; 3) moderatoren sørger for, at samtalen ikke bliver ved et emne for længe eller bevæger sig for hurtigt, og at alle taler. Trænerne griber kun ind, når det er nødvendigt.
Flipped Classroom	Det er en pædagogisk tilgang, hvor de traditionelle elementer i lektionen undervist af underviseren er vendt om: det primære undervisningsmateriale studeres af eleverne derhjemme og derefter arbejdes videre med i sessionen.
Stationslæring	Ved hjælp af stationslæringsmetoden bearbejdes indholdet individuelt og behovsorienteret. Underviseren udarbejder en læringsstation for hver applikationskomponent, hvor arbejdsopgaver og arbejdsmaterialer er tilgængelige. Eleverne kan vælge de stationer, der interesserer dem med hensyn til indhold, og som de vurderer som vigtige for deres individuelle anvendelse. Træneren er altid tilgængelig for spørgsmål. Eleverne tager noter og vil senere også have adgang til materialer / prøver osv. på alle stationer. De kan selv vælge deres læringsvej fra station til station.

Bord 3 – Identifikation og kort beskrivelse af de metoder, der tages i betragtning heri

Modul 1: Information og datafærdighed

Det første modul vil introducere dig til online-søgningsprocedurerne, og fokuserer også på, hvordan du vurderer informationen, hvordan du opbevarer, henter den og bruger den ansvarligt.

Bemærk venligst, at praktiske aktiviteter beskrevet i hver enhed kan indebære støtte fra en erfaren træner. Selvom oplysningerne i manualen er skrevet på en måde, der er let at forstå, kan nogle handlinger, der støder op til de præsenterede oplysninger, kræve overvågning og støtte fra erfarne personer.

Modul 1	**Information og datafærdighed**		
Varighed	25 timer		
Mål	At søge pålidelig information online ved hjælp af forskellige browsere og søgemaskiner Udfør onlinesøgning på en sikker og sikker måde Identificer mulige falske nyheder og vildledende oplysninger på websteder Organiser, gem og hent information		
Enheder	1.1 Gennemse, søge og filtrere data, information og digitalt indhold	1.2 Evaluering af data, information og digitalt indhold	1.3 Håndtering af data, information og digitalt indhold
Træningsorganisation	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring
Varighed	9 timer	8 timer	8 timer

Bord 4 – Global struktur af modul 1 – Information og datafærdighed.

1.1. Gennemse, søge og filtrere data

Enhed 1.1	Gennemse, søge og filtrere data, information og digitalt indhold
Varighed	9 timer
Mål	At bruge forskellige browsere og søgemaskiner til onlinesøgning; For at udføre en onlinesøgning på et specifikt emne ved at vælge pålidelige informationskilder; At identificere mistænkelige websteder og misinformation; For at gemme og hente data såsom dokumenter, billeder, websteder; At administrere det digitale miljø under hensyntagen til privatlivsindstillinger og fortrolighed
Indhold	1.1.1 Hovedbegreber: IT, IKT og internet 1.1.2 Introduktion til søgning online 1.1.3 Beskyttelse ved brug af IKT 1.1.4 Praktiske aktiviteter
Ressourcer	Træningsmanual Computer med internetadgang Flipover papirer Markører Casestudie 1 og 2
Træningsmetoder	Præsentation af træner Gruppeøvelse Diskussion / Debat Arbejde i par/små grupper Præsentation af deltagere

Bord 5– Kompetenceenhedens opbygning 1.1. - Gennemse, søge og filtrere data fra Modul 1 – Information og datafærdighed.

1.1.1. Hovedbegreber: IT, IKT og internet

For at introducere dig til dette modul vil vi gerne præsentere to hovedbegreber, som du sikkert hører meget, når du taler om computerteknologi. Disse er:

IT (informationsteknologi) - omfatter al den teknologi, som vi bruger til at indsamle, behandle, beskytte og opbevare information. Det refererer til hardware, software (computerprogrammer) og computernetværk.

IKT (informations- og kommunikationsteknologi) - dette koncept involverer overførsel og brug af alle former for information. IKT er grundlaget for økonomi og en drivkraft for sociale forandringer i det 21. århundrede. Afstand er ikke længere et problem, når det kommer til at få adgang til information; for eksempel er arbejde hjemmefra, fjernundervisning, e-banking og e-forvaltning nu muligt fra ethvert sted med en internetforbindelse og en computerenhed.

Tage til efterretning:
IKT omfatter alle tekniske midler, der bruges til at håndtere information og facilitere kommunikation, herunder computere, netværkshardware, kommunikationslinjer og al nødvendig software. Med andre ord består IKT af informationsteknologi, telefoni, elektroniske medier og alle typer processer og overførsel af lyd- og videosignaler samt alle kontrol- og styringsfunktioner baseret på netværksteknologier.

Internettet
Internet ("netværk af alle netværk") er et globalt system bestående af indbyrdes forbundne computere og computernetværk, som kommunikerer ved hjælp af TCP/IP-protokoller. Selvom det i sin begyndelse opstod ud fra behovet for simpel dataudveksling, påvirker det i dag alle samfundets domæner, for eksempel:

- **Økonomi**: Internetbank (betaling af regninger, overførsel af midler, adgang til konto, adgang til kreditgæld osv.), elektronisk handel (aktier, forskellige varer, intellektuelle tjenester osv.) osv.
- **Socialisering**: sociale netværk, fora...
- **Information**: nyhedsportaler, blogs mm.
- **Sundhedspleje**: diagnosticering af sygdom, lægeundersøgelser (for personer, der bor på en ø eller andre fjerntliggende steder, nogle undersøgelser, der kræver en specialist, kan udføres eksternt), aftaler om lægeundersøgelser, udveksling af medicinske data mellem hospitaler og institutter, kirurgi og fjernovervågning af operationer
- **Uddannelse**: online universiteter med webinarer (web + seminar), websteder med tutorials, ekspertrådgivning, online træning osv.

Internettet har virkelig mange applikationer og en enorm social indvirkning. Den måske vigtigste egenskab er informationsudveksling, fordi informationsudveksling mellem mennesker muliggør samarbejde, samarbejde mellem ligesindede fører til ideer og handlinger i det virkelige liv og koordinerede handlinger af mennesker resulterer i social forandring.

Nu hvor du lærte mere om teknologi og internettets potentiale til at ændre verden, så tag et øjeblik til at tænke over, hvordan det kan påvirke dig og dit personlige liv.

Du undrer dig måske lige nu... ok, denne idé om at forbinde med andre på en så nem måde lyder fantastisk, men hvordan bruger jeg disse værktøjer? Det er det første emne i denne manual: at søge online og lære at gennemse, søge og filtrere information.

1.1.2. Introduktion til søgning på nettet

Evnen til at søge efter information online er en af de vigtigste digitale færdigheder, du kan besidde. Det giver dig mulighed for hurtigt at finde det, du leder efter, uden at skulle gennemsøge sider med irrelevante resultater.

Det vigtigste værktøj i denne proces er søgemaskinen, som er en specialiseret hjemmeside, der søger efter information på tværs af internettet. Du har sikkert hørt om de mest populære, inklusive Google, Yahoo! og Bing, og selvom hver af dem er nyttige, kan de også give forskellige resultater.

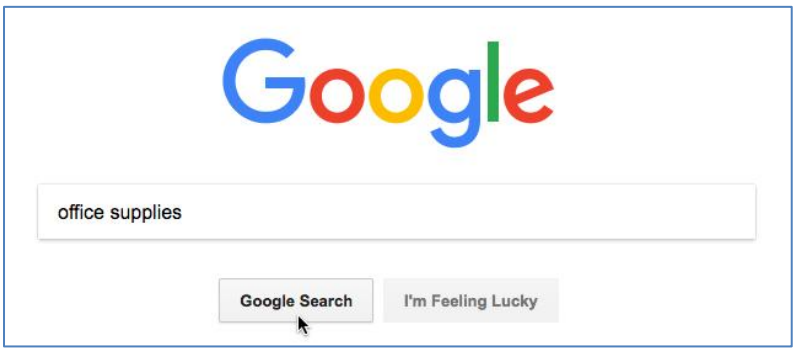
Samlet set er Google den mest populære søgemaskine. Det er faktisk så populært, at det endda er blevet et almindeligt udsagnsord, som når nogen siger: "Jeg googler adressen lige nu".

Sådan begynder du at søge

For at starte en søgning skal du klikke på en **browser**. En browser er en software, der gør det muligt for en computerbruger at finde og se oplysninger på internettet, og der er forskellige tilgængelige for brugerne. Internet Explorer, Mozillas Firefox og Chrome er blot nogle af dem, og du finder dem som regel nederst på din computers skrivebord.

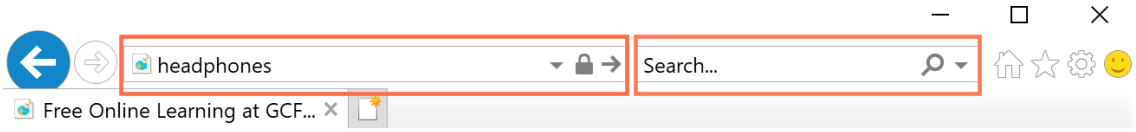
Figur 3 – Ikoner for nogle browsere.

Gå derefter til søgemaskinens hjemmeside, for eksempel **google.com**, og skriv dine søgeord i tekstfeltet. For at se dine resultater kan du trykke på Enter-tasten, eller du kan klikke på et ikon, såsom Google Søg-knappen eller et forstørrelsesglas.



Figur 4 – Googles hjemmeside.

Afhængigt af din browser kan du muligvis udføre en søgning direkte fra browserens grænseflade. For eksempel kan du i Chrome indtaste dit søgeord direkte i adresselinjen. I Internet Explorer (billedet nedenfor) kan du bruge enten adresselinjen eller den indbyggede søgelinje til at starte en søgning.



Figur 5 – Chrome-hjemmeside.

Søgestrategier

Med nogle få grundlæggende søgestrategier kan du som regel finde næsten alt, hvad du ønsker. Det er ligegyldigt, om du bruger Google eller en anden søgemaskine, fordi disse teknikker er effektive, uanset hvor du søger.

- **Hold det simpelt:**Gør dine søgninger korte ved at fokusere på søgeord, og hold derefter antallet af disse søgeord på et minimum. På denne måde er der større sandsynlighed for, at du får relevante resultater.
- **Overvej forslag:** Når du indtaster dit udtryk, vil søgemaskiner foreslå de mest populære resultater, der involverer udtrykket, så vær ikke bange for at vælge et, da de ofte kan give dig masser af nye ideer.
- **Brug naturligt sprog:**Du behøver ikke bruge komplicerede ord eller sætninger for at få resultater. Søgemaskiner kan genkende det sprog, du naturligt bruger i din hverdag, så du er velkommen til at prøve, hvad der falder dig ind.

Afhængigt af din søgning kan formatet på dine resultater variere baseret på, hvad søgemaskinen mener vil være mest nyttigt. Det betyder, at dine resultater kan omfatte kort, en del af en Wikipedia-artikel, lister og mere.
Søgemaskiner kan finde mange andre typer indhold ud over websider. Med kun et klik eller to kan du også søge efter billeder, videoer, nyheder og meget mere.
Inden du starter din onlineoplevelse, vil vi gerne henlede din opmærksomhed på noget af yderste vigtighed: **indstillinger for online sikkerhed og privatliv.**

1.1.3. Beskyttelse ved brug af IKT

Informationssikkerhed er defineret som bevarelse af informationsfortrolighed, integritet og tilgængelighed.
Informationssikkerhedsforanstaltninger er reglerne for databeskyttelse på fysisk, teknisk og organisatorisk niveau. Brugergodkendelse involverer brugeridentifikation, så enkeltpersoner kan få adgang til et bestemt indhold (data). For at tjekke din e-mail via browser, dvs. få adgang til en konto, er det nødvendigt at indtaste et brugernavn og en adgangskode. Hvis de nødvendige oplysninger er indtastet korrekt, gives der adgang. Adgangskoder bør af sikkerhedsmæssige årsager holdes fortrolige. En adgangskode er en nøgle (som en nøgle til at få adgang til dit hjem eller en bil), der giver adgang.
Da du ikke ville dele din lejlighed eller bilnøgler med hvem som helst, bør du heller ikke dele din adgangskode. Mange mennesker har i dag sikkerhedsdøre til hjemmet med låse, hvis nøgler er svære at kopiere, med det formål at blokere for uautoriseret indtrængen i hjemmet. Adgangskoder bør oprettes med samme forsigtighed. Jo mere kompleks din adgangskode er, jo sværere vil den være at bryde igennem (knække den), derfor er det mindre sandsynligt, at nogen får uautoriseret adgang til dine data.

Når du vælger en adgangskode, er det tilrådeligt at bruge tegnsætning, tal og en blanding af store og små bogstaver. En minimumlængde på 8 tegn anbefales (kortere adgangskoder er nemmere at bryde igennem).
Fra tid til anden er det nødvendigt at ændre adgangskoden. På den måde mindskes muligheden for dets påvisning.

Nogle af de mest almindelige fejl ved valg af adgangskoder er:

- bruge ord fra en ordbog
- adgangskoder baseret på personlige oplysninger, såsom navn eller fødselsdato, ansættelsessted osv.
- tegn, der følger rækkefølgen givet på et tastatur: 123, qwert osv.

Hjemmesidens sikkerhed: for at se, om et websted er sikkert at besøge, kan du tjekke for sikkerhedsoplysninger om webstedet. Tjek til venstre for webadressen for sikkerhedsstatus:

- Hvis du ser et låseikon ved siden af et websteds adresse, betyder det, at trafikken til og fra webstedet er krypteret.

Det er også verificeret, hvilket betyder, at virksomheden, der driver siden, har et certifikat, der beviser, at de ejer det. Ved at vælge låseikonet kan du se flere oplysninger om webstedet, såsom hvem der ejer det, og hvem der har bekræftet det.
Hvis du ikke kan se et låseikon, din forbindelse er ikke privat, og al trafik kan blive opsnappet.

Figur 6 – Identifikation af låseikonet.

Personlige oplysninger – et par ting at huske på!

Du skal være forsigtig med, hvor mange personlige oplysninger du afslører online. At dele din adresse, telefonnummer, fødselsdag og andre personlige oplysninger kan betyde, at du har en større risiko for identitetstyveri, stalking og chikane. Dette inkluderer oplysninger, du poster på sociale medier.
Cyberkriminelle kan sammensætte din identitet ud fra oplysninger, der er offentligt tilgængelige om dig, så tænk over, hvilke oplysninger du deler online.

Derfor er her et par ting at overveje, når du bruger internettet:

- Brug en separat e-mailadresse til shopping, diskussionsgrupper og nyhedsbreve. Hvis du har brug for det, kan du derefter ændre denne adresse uden at forstyrre online forretningsaktiviteter.
- Del kun din primære e-mailadresse med personer, du kender.
- Hvis du bruger sociale medier, skal du justere dine privatlivsindstillinger for at kontrollere mængden og typen af information, du deler.
- Når du opretter en konto, tag dig tid til at sætte dig ind i de sociale mediers privatlivspolitikker.
- Foretag kun online køb fra virksomheder, der har en klar privatlivspolitik og sikre betalingsmuligheder
- Tænk dig om, før du udfylder onlineformularer, og vær forsigtig med, hvem og hvordan du deler dine oplysninger. Spørg dig selv, skal jeg virkelig give mine oplysninger til dette websted?

1.1.4. Praktiske aktiviteter

Efter hver teoretisk beskrivelse af indholdet foreslår vi nogle gruppedynamikker for at forbedre læringen. Disse aktiviteter beskrives trin for trin.

Når man leverer træning, er det vigtigt, at trænere og elever føler sig godt tilpas i gruppen, så de føler sig glade for at dele erfaringer, spørgsmål og så videre. Jo mere folk føler sig godt tilpas med deres kolleger, jo bedre er læringsoplevelsen. Derfor foreslår vi, at hver aktivitet starter med en isbryder, om muligt noget sjovt, som giver folk mulighed for at præsentere sig selv for gruppen uden at føle sig intimideret.

På præsentationsstadiet vil underviseren måske invitere folk til at dele, hvad de gerne vil lære, hvilket dyr de gerne vil være, hvad er deres yndlingsret, hvilken farve er deres tandbørste og ethvert andet emne, da det er noget, der ikke er for personligt.

Trin 1: Isbryder "Jeg er den eneste"

Alle spreder sig rundt i lokalet og laver en lukket cirkel. Træner forklarer, at en bold vil gå rundt og stoppe på hver person i cirklen. Den, der har bolden, skal sige deres navn og én ting, de er de eneste, der ved eller gør i gruppen. De kan også tale om en udsøgt interesse eller smag. Hvis et andet medlem af gruppen deler den samme færdighed, skal den person, der talte, finde noget andet, der er anderledes.

Bolden behøver ikke at følge en ordre, så folk kan smide den til enhver i gruppen, bare sørge for at hver person har en chance for at tale.

Du kan justere denne isbryder til et online-format ved at bede folk om at nominere en kollega til at tale i stedet for at kaste en bold.

Trin 2: Brainstorming starter

For at introducere emnet onlinesøgning, men også for at få en idé om, hvor folk er i form af almindelig viden, start denne enhed med en brainstorm.

Sørg for at have en tavle klar til at registrere alles input. Hvis aktiviteten afvikles online, kan du bruge en online platform til at støtte med tilmelding (f.eks.https://padlet.com) eller endda dele et word-dokument med gruppen, hvor du bare kan skrive deres svar.

Informer deltagerne om, at der ikke er rigtige/forkerte svar, fordi tanken er at dele med gruppen, hvad vi allerede ved/måske ikke ved. Mulige spørgsmål:

- Hvad er en onlinesøgning?
- Hvordan kan denne viden være nyttig i vores daglige liv?
- Hvordan ender information på internettet?
- Hvilken slags risici kan man støde på, når man søger på nettet?

Trin 3: Onlinesøgning – hands on!

Vis deltagerne forskellige webbrowsere: Google Chrome, Safari, Mozilla Firefox, Edge, Internet Explorer, og forklar, at disse er softwareprogrammer til at få adgang til World Wide Web og navigere gennem forskellige sider; vise deltagerne, hvor de kan finde browserne på en computer; (10 minutter)

Du kan også bruge følgende selvstudie for at introducere emnet for, hvordan man bruger en søgemaskine: https://edu.gcfglobal.org/en/internetbasics/using-search-engines/1/

Underviseren viser, hvordan man søger efter "organisk gødning" (dette er et eksempel, men det er tilrådeligt, at du vælger et meningsfuldt emne for din gruppe); Vis gruppen, hvordan man ser på forskellige sider, og hvordan man bruger forskellige "søgeudtryk"; (10 minutter)

Inviter nu hver deltager til at søge online efter information om farerne ved falske nyheder og nedskriv tre hovedfakta, de har fundet; (20 minutter)

Gruppediskussion: hver deltager præsenterer resultaterne af deres søgning. (20 minutter)

Trin 4: Analyse, lagring og præsentation af information

Hav en liste over forskellige emner klar, som deltagerne kan udforske online. Eks: mental sundhed under pandemien, de bedste opskrifter i verden, ekstremsport, biernes betydning, træsygdomme, industriel revolution, robotter inden for teknologi, sund livsstil osv.

Bed gruppen om at organisere sig i par og vælge et emne at arbejde med. Hovedmålet i denne aktivitet er 1) at kompilere pålidelig information om det valgte emne, 2) vælge og gemme informationen på skrivebordet (i en

mappe oprettet af eleven) og 3) oprette en kort præsentation (10 minutter lang) sikre, at de har brugt troværdige kilder. Elever skal registrere de anvendte hjemmesider og referencer, da dette vil blive vurderet til sidst.

For de elever, der måske ikke er i stand til at bruge software til at arbejde med præsentationen, skal underviseren sørge for flipover-papir og markører. Selvom de ikke bruger computeren til at præsentere information, skal de være i stand til at søge i billeder, grafik eller videoer for at illustrere deres søgning og gemme dem i deres skrivebordsmappe. (4 timer)

Når denne opgave er færdig, skal hver gruppe præsentere arbejdet for kollegerne. (90 minutter)

Trin 5: Privatlivsindstillinger online

Giv eleverne Case Study 1 og 2. Derudover vil du måske invitere dem til at se et hurtigt selvstudie om privatliv og sikkerhed i Chrome: https://www.youtube.com/watch?v=zMXI6waGFp4

- Del eleverne op i to grupper for at arbejde med hver case. De skal læse og besvare spørgsmålene, understøttet af online information om cybersikkerhed. (30 minutter).
- Hver gruppe laver et faktaark[7], der peger på ti trin til at undgå brud på privatlivets fred, mens du bruger internettet (20 minutter)
- Gruppedebat (40 minutter)

[7] Praktikanter kan gøre dette på computeren eller et flipover-papir, afhængigt af deres allerede eksisterende digitale færdigheder.

Casestudie 1 - Jane

Læs følgende situation og diskuter i din gruppe, hvad der skete, og besvar spørgsmålene nedenfor for at styre debatten. Skriv derefter hovedkonklusionerne ned, så du kan præsentere dine ideer for gruppen.

"Jane logger på internettet og forbereder sig på, hvad de fleste ville betragte som en typisk, harmløs internetoplevelse. Jane køber noget tøj til sig selv og sine to- og femårige børn på et eksklusivt stormagasins websted. Hun følger derefter med en udvidet gennemgang af et websted med vægttabsplaner. Selvom de fleste ville betragte denne browsing-oplevelse som en samling verdslige transaktioner, anser en kyndig direkte marketingmedarbejder med evnen til skjult overvåge disse aktiviteter, at den opnåede information er uvurderlig. Så overraskende som det kan være for mange websurfere, er det ganske muligt at samle en alarmerende detaljeret profil af Jane, uden hendes viden eller samtykke, med en enkelt browsing-aktivitet som den tidligere skitserede. Selvom dette scenarie kræver nogle slutninger, en markedsføringsprofil af Janes transaktioner kan udvikle sig som følger: Jane er mor med to små børn, køber nogle eksklusive varer og er alvorligt bekymret over sin vægt og helbred. Baseret på hende vil en købmand eller sælger måske sende Jane-reklamer, e-mails, bannere, reklamer eller pop-up-reklamer, der tilbyder dyrt træningsudstyr til hjemmet. Udstyret ville give hende mulighed for at blive hjemme med sine børn, hjælpe med hendes fitnessmål og være overkommelig baseret på hendes observerede forbrugsmønster. En annonce for træningsudstyr generer måske slet ikke Jane. Faktisk kan hun faktisk være interesseret i hjemmetræningsudstyr i stedet for en anden annonce, der ville være blevet tilfældigt lagt op på hendes computerskærm, mens hun surfede på nettet. Imidlertid,

Groemminger, BK (2003). Personligt privatliv på internettet: bør det være en ret til cyberspace[8].

1) **Hvilke privatlivsindstillinger eller handlinger kunne Jane tage for at undgå, at hendes oplysninger spredes gennem kommercielle virksomheder?** (Mulige svar nedenfor)
- Hun bør være opmærksom på cookies-tilladelser ved kun at tillade de nødvendige
- Hun kunne slette søgehistorikken, når den er færdig, eller logge ind som anonym – dette er især relevant, hvis hun bruger en offentlig computer
- Hun skal logge ud af sin e-mail eller andre konti, hun måske har logget ind.

2) **Hvilken slags sikkerhedsforanstaltninger vil du tage i betragtning, når du handler online?** (Mulige svar nedenfor)
- Tjek hjemmesidens sikkerhed - se om det er en sikker forbindelse
- Opret et virtuelt kort med et bestemt beløb
- Brug troværdige platforme til betalinger som PayPal
- Sørg for, at du kører en virusscanning, og at din computer er sikker
- Undgå at bruge en offentlig netværksforbindelse, mens du handler

Casestudie 2 - Mary

Læs følgende situation og diskuter i din gruppe, hvad der skete, og besvar spørgsmålene nedenfor for at styre debatten. Skriv derefter hovedkonklusionerne ned, så du kan præsentere dine ideer for gruppen.

Mary er 22 år gammel, og hun er meget vidende om sociale netværk, da hun kalder sig selv "en influencer". Hun mener, at regelmæssig motion og god ernæring er grundpillerne for en sund livsstil, og hun skriver mange indlæg og forslag på Instagram om det. Hun har nået lidt over 10000 følgere, og hun er meget stolt over det. For nylig skrev nogle mennesker til hende og klagede over, at de var blevet ramt af et cyberangreb på grund af beskeder sendt i hendes navn. I begyndelsen ved hun ikke, hvordan hun skal forklare dette, men så indser hun, at hun er blevet hacket. For to dage siden modtog hun en besked om, at hun havde vundet en online konkurrence. I begyndelsen fandt hun beskeden lidt mistænkelig, da hun ikke kunne genkende afsenderen, men så klikkede hun på linket og udfyldte en formular med personlige oplysninger. Da der ikke var nogen præmie, så fandt hun ud af, at det var et fupnummer. Da hun var klar over det, udsendte hun en advarsel på sociale medier, der informerede alle om ikke at åbne beskeder fra hende.

1) **Hvad kunne Mary ellers gøre, når hun indså, hvad der skete?**(Mulige svar nedenfor)
   - nulstil adgangskoderne (e-mail, telefon, sociale medier, bank osv.), og sørg for, at disse adgangskoder er stærke (minimum 8 tegn med store bogstaver, tal osv.)
   - sikre, at anti-virussen er opdateret / kør en virusscanning
   - sikkerhedskopiere hendes data
   - tag enheden til en it-professionel

2) **Hvad kunne Mary gøre for at undgå denne situation?** (Mulige svar nedenfor)
   - Hun skulle have tjekket to gange afsenderen og aldrig åbne beskeden/linket, hvis det var mistænkeligt
   - Hun skulle have tjekket hjemmesidens adresse og se, om den var markeret som farlig

1.2. Evaluering af data, information og digitalt indhold

Enhed 2 er relateret til evaluering af information, vurdere dens troværdighed og kilder.

Enhed 1.2	Evaluering af data, information og digitalt indhold
Varighed	8 timer
Mål	At analysere og vurdere troværdigheden af information online At tage skridt til at evaluere forskellige informationskilder At forstå hver enkelts ansvar, når de deler misinformation online At være opmærksom på, hvordan personlige værdier og vurderinger påvirker forståelsen af information
Indhold	1.2.1 Hvordan man vurderer kilder og information online 1.2.2 Evaluering af dine kilder 1.2.3 Evaluering af websteder 1.2.4 Fakta-tjek hjemmesider 1.2.5 Praktiske aktiviteter
Ressourcer	Træningsmanual, computere med internetadgang, sandt eller falsk kort
Træningsmetoder	Præsentation af træner Gruppeøvelse Diskussion / Debat Arbejde i par/små grupper Præsentation af deltagere Medievalg

Bord 6- Kompetenceenhedens opbygning 1.2. Evaluering af data, information og digitalt indhold i Modul 1 – Information og datafærdighed

1.2.1. Hvordan vurderer man kilder og information online?

Da du nåede denne del af manualen, har du allerede en klar idé om, hvilken information du kan finde online: stort set alt! Denne bekræftelse introducerer den næste enhed, hvor du lærer at vurdere data, så du er i stand til at lede efter pålidelige kilder og derfor bidrage til at dele faktuel information online.

I modsætning til lignende oplysninger, der findes i aviser eller tv-udsendelser, er information tilgængelig på internettet ikke reguleret for kvalitet eller nøjagtighed. Derfor er det særligt vigtigt for den enkelte internetbruger at vurdere ressourcen eller informationen. Husk, at næsten alle kan udgive alt, hvad de ønsker på nettet. Det er ofte svært at bestemme forfatterskab til webkilder, så**det er virkelig dit ansvar at bedømme**

nøjagtigheden af dine kilder. På trods af de vigtigste ressourcer til at gøre det er din dømmekraft og ræsonnement, er der et par handlinger, der kan hjælpe dig med at øge oddsene til fordel for pålidelig information.

Stil dig selv disse spørgsmål, før du bruger ressourcer fra internettet:

1. Hvem er forfatteren? Er forfatteren kvalificeret til at skrive om emnet? Hvis det er en organisation, er den så troværdig? Hørte jeg om det?
2. Hvad er formålet med siden? Hvem er den tiltænkte målgruppe?
3. Er informationen og sproget objektiv, upartisk og fri for følelsesskabende udtryk?
4. Er de faktuelle kilder anført, så oplysninger kan verificeres?
5. Er oplysninger understøttet af beviser?
6. Hvor gammel er denne information? Hvornår blev siden sidst opdateret?

Sidst men ikke mindst…Tjek dine følelser!

Vær opmærksom på, hvornår en titel har magten til at ændre din følelsesmæssige tilstand. Dette er ikke kun en meget gammel teknik til at tiltrække din opmærksomhed, men den er blevet brugt som clickbait til spredning af falske nyheder. Vores normale tilbøjelighed er at ignorere verifikationsbehov, når vi reagerer stærkt på indhold, og forskere har fundet ud af, at indhold, der forårsager stærke følelser, spredes hurtigst gennem vores sociale netværk (Matthew Shaer, 2014). Så,**læse ud over overskrifterne**!

1.2.2. Evaluering af dine kilder

I din søgen efter information står du til sidst over for udfordringen med at evaluere de ressourcer, du har fundet, og udvælge dem, du vurderer, er mest passende til dine behov. Undersøg hver informationskilde, du finder, og vurder kilder ved hjælp af følgende kriterier, også kendt som**TAARP metode:**

T – Aktualitet Dine ressourcer skal være nye nok til dit emne. Hvis dit papir handler om et emne som kræftforskning, vil du gerne have den nyeste information, men et emne som Anden Verdenskrig kunne bruge information skrevet i et bredere tidsinterval.
A – Myndighed Kommer oplysningerne fra en forfatter eller organisation, der har autoritet til at tale om dit emne? Er oplysningerne blevet peer-reviewet? (Du kan bruge Ulrichsweb til at afgøre, om et tidsskrift er peer-reviewed). Anfører de deres legitimationsoplysninger? Sørg for, at der er tilstrækkelig dokumentation til at hjælpe dig med at afgøre, om publikationen er pålidelig, herunder fodnoter, bibliografier, krediteringer eller citater.
A – Publikum Hvem er de tiltænkte læsere, og hvad er publikationens formål? Der er forskel på et blad skrevet til den brede offentlighed og et tidsskrift skrevet til professorer og eksperter på området.
R – Relevans Relaterer denne artikel dit emne? Hvilken sammenhæng kan der skabes mellem den information, der præsenteres, og dit speciale? En nem måde at tjekke for relevans er ved at gennemgå abstraktet eller resuméet af artiklen, før du downloader hele artiklen.
P – Perspektiv Fordomsfulde kilder kan være nyttige til at skabe og udvikle et argument, men sørg for at finde kilder til at hjælpe dig med at forstå den anden side også. Ekstremt partiske kilder vil ofte give oplysninger forkert, og det kan være ineffektivt at bruge i dit papir.

1.2.3. Evaluering af hjemmesider

Hjemmesider skaber en interessant udfordring i at evaluere troværdighed og anvendelighed, fordi ikke to hjemmesider er skabt på samme måde. TAARP-metoden beskrevet ovenfor kan bruges, men der er yderligere ting, du vil overveje, når du ser på en hjemmeside:

Udseendet og følelsen af hjemmesiden- Pålidelige websteder har normalt et mere professionelt udseende end personlige websteder.

Webadressen til dine resultater- .com, .edu, .gov, .net og .org betyder alle faktisk noget og kan hjælpe dig med at evaluere hjemmesiden!

Informational Resources are those which present factual information. These are usually sponsored by educational institutions or governmental agencies. (These resources often include **.edu** or **.gov**.)

Advocacy Resources are those sponsored by an organization that is trying to sell ideas or influence public opinion. (These resources may include **.org** within the URL.)

Business or Marketing Resources are those sponsored by a commercial entity that is trying to sell products. These pages are often very biased, but can provide useful information. (You will usually find **.com** within the URL of these resources.

News Resources are those which provide extremely current information on hot topics. Most of the time news sources are not as credible as academic journals, and newspapers range in credibility from paper to paper. (The URL will usually include **.com**.)

Personal Web Pages/Resources are sites such as social media sites: blogs, Twitter pages, Facebook, etc. These sources can be helpful to determine what people are saying on a topic and what discussions are taking place. Exercise great caution if trying to incorporate these sources directly into an academic paper. Very rarely, if ever, will they hold any weight in the scholarly community.

Er der reklamer på siden?- Annoncer kan indikere, at oplysningerne kan være mindre pålidelige.

Tjek links på siden- Ødelagte eller forkerte links kan betyde, at ingen tager sig af siden, og at andre oplysninger på den kan være forældede eller upålidelige.

Tjek hvornår siden sidst er blevet opdateret- Datoer, hvor sider sidst blev opdateret, er værdifulde ledetråde til dens valuta og nøjagtighed.

1.2.4. Fakta-tjek hjemmesider

Heldigvis kan du også bruge et faktatjek-websted, hvor du kan tjekke yderligere, om de oplysninger, du fandt, er blevet markeret som falske. Derudover kan du spørge en bibliotekar. Her er en liste over nogle faktatjeksider (afhængigt af dit hjemland, kan det være interessant at kigge efter faktatjeksider på nationale nyheder. Dem vi præsenterer er for det meste amerikanske):

- FactCheck.org - https://www.factcheck.org/
- PolitiFact: at finde ud af sandheden i politik - https://www.politifact.com/truth-o-meter/
- Urban Legends: Politik -https://www.snopes.com/fact-check/category/politics/
- Sandhed eller fiktion - https://www.truthorfiction.com/
- Observador Fact-Check (Portugal) -https://observador.pt/seccao/observador/fact-check/

1.2.5. Praktiske aktiviteter

Trin 1: Sandt eller falsk?

For at introducere emnet for, hvordan man vurderer rigtigheden af oplysninger, vi støder på online, skal du starte med et hurtigt sandt eller falsk spil. Du skal forberede nogle Sande/Falske kort tidligere og dele eleverne op i grupper på tre. Du vil præsentere nogle bekræftelser relateret til emnet, og hver gruppe skal vise det sande eller det falske kort, alt efter deres svar. Du kan rette svarene og give nogle oplysninger om emnerne, mens du går.

Liste over bekræftelser:

	Bekræftelse	T/F
1	Alle oplysninger, der er lagt ud på nettet, er pålidelige.	Falsk
2	Alle kan tilføje oplysninger online, selv på leksika	Rigtigt
3	Der er måder at kontrollere oplysningernes troværdighed på.	Rigtigt
4	Der er et fænomen med "falske nyheder" rundt om i verden.	Rigtigt
5	For at spotte falske nyheder kunne man tjekke webdomænet.	Rigtigt
6	Jo mere noget deles, jo mere sandsynligt er sandheden.	Falsk
7	At tjekke nyhedsdatoen er ikke noget, der er værd at overveje.	Falsk
8	Personlige værdier kan påvirke ens opfattelse af sandheden.	Rigtigt
9	Det er normalt meget nemt at identificere en falsk ny.	Falsk

10	Der er tilgængelige faktatjeksider.	Rigtigt

Bord 7 – Liste over bekræftelser og korrekt svar.

Trin 2: Hvordan spredes misinformation?

For at understøtte indlæringen af, hvordan man evaluerer data online, kan du præsentere en hurtig video, der viser, hvordan falske nyheder spredes.

Forslag: https://www.youtube.com/watch?v=cSKGa_7XJkg

Herefter kan hver praktikant medføre deres egen søgning for at finde to nyheder, der sandsynligvis er sande, og to nyheder, der sandsynligvis er falske. Under hensyntagen til informationen givet af underviseren om, hvordan man evaluerer datas pålidelighed, bliver eleverne nu nødt til at bruge nogle af disse strategier for at udvælge information og være i stand til at forklare kolleger, hvilke strategier de har brugt.

Trin 3: Fortælleaktivitet

Den følgende historie fortæller om to landmænd, der stræber efter at styre deres forretning i en lille landsby. Den ene er meget dygtig til digitale værktøjer, men den anden er ikke særlig dygtig til det. Historien fremhæver potentialet ved at bruge internettet til at sprede rygter og falske nyheder. Hovedmålet med historien er at fremkalde personlige tanker om, hvad der er falsk nyt, og hvor let nogen kan gøre det, men også at tænke på den indflydelse, de kan have på vores daglige liv og verden over.

Vi sigter også efter at fremme en debat om fordelene ved internettet, og hvordan det kan være nyttigt at hjælpe os med at nå information hurtigt, støtte os i at komme i kontakt med andre, der måske kan hjælpe osv. Vi foreslår underviseren at præsentere følgende historie :

Der var to mænd i en lille landsby: Robert og Peter. Begge var meget hårdtarbejdende mennesker, der drev store gårde og deres egen virksomhed. De plejede at tale meget stolte om de produkter, de sælger til markederne, da de altid har fulgt procedurer for at garantere høje kvalitetsstandarder.

Peter og Robert har altid været naboer og kender hinanden i over 10 år nu. Vi kan dog ikke sige, at deres forhold altid har været godt, da de altid har konkurreret om de faste kunder i landsbyen og den lille by i nærheden. De mener, at der ikke er plads til begge i branchen på så lille et område.

På en af sine morgenvandringer oplever Robert, at Peter er meget bekymret over sine plantager, da salaterne er ødelagt af, hvad der ser ud til at være en pest. Han er ked af, at han ikke har bemærket det tidligere og klager over, at der i denne uge ikke vil være salat at sælge på byens marked. Han er også bekymret for, at hvis kunderne finder ud af, hvad der skete, kan de se ham som inkompetent og miste tillid til kvaliteten af hans produkter. Desuden ved han ikke, hvordan han skal håndtere denne pest, da det ser ud til at være en helt ny virus, han aldrig har set før.

I mellemtiden tænker Robert på, at denne uheldige begivenhed faktisk kan være en chance for ham til at nedlægge sin nabos forretning én gang for alle! Så han beslutter sig for at oprette en Facebook-profil for en person, der angiveligt har købt Peters produkter og er meget utilfreds. For at dække løgnen endnu bedre, fandt Robert nogle billeder online og tilføjede dem i profilen, som om de var billeder af Peters dårlige produkter. Så begynder han at sende venskabsanmodninger til folk i landsbyen, og beskeden bliver hurtigt spredt rundt.

Et par dage senere indser Peter, at hans fortjeneste er faldet markant, selv i salget af andre produkter, som ikke var ramt af pesten. Han har dog ingen idé om, hvad Robert har lavet på internettet bag hans ryg...

Foreslåede spørgsmål til gruppedebat:

- Hvorfor tror du, at Peters fortjeneste begyndte at falde?
- Hvis du var Peters klient, hvordan tror du så, at du kunne have det med at se billeder af rådden salat? Ville du stadig købe hans produkter?
- Hvor let tror du, det er at sprede rygter og misinformation online?
- I betragtning af den indflydelse falske nyheder havde på Peters forretning, hvordan tror du, det kan påvirke politik for eksempel eller folkesundhedsspørgsmål relateret til covid-19? Kan du komme i tanke om nogen nyheder om covid-19, du måske har hørt og måske ikke er sande?
- Forestil dig nu, at du var i Peters sko... ville du have brugt internettet til at hjælpe dig

1.3. Håndtering af data, information og digitalt indhold

Enhed 1.3	Håndtering af data, information og digitalt indhold
Varighed	8 timer
Mål	Til at gemme og gemme oplysninger ved hjælp af forskellige enheder For at administrere, lokalisere og hente data For at forstå reglerne om ophavsret og licens At være opmærksom på databeskyttelseslovgivningen
Indhold	1.3.1 Enheder til at gemme og hente oplysninger 1.3.2 Ophavsret og databeskyttelse 1.3.3 Praktiske aktiviteter
Ressourcer	Træningsvejledning, computere med internetadgang, en hat, stykker papir, 1 til 5 skala (du kan bruge 5 papirer nummereret 1 til 5), flipover-papirer, blu-tack eller andet materiale til at klæbe papirer på væggen, farvede tuscher, stole, bord, ske, horn eller enhver genstand for at lave en alarmlyd Adgang til kollaborativ læringsplatform, hvis det gøres online (f.eks.: LAMS, Padle)
Træningsmetoder	Præsentation af træner Gruppeøvelse Diskussion / Debat Arbejde i par/små grupper Præsentation af deltagere Kooperativ læring

Bord 8- Kompetenceenhedens opbygning 1.3. Håndtering af data, information og digitalt indhold i Modul 1 – Information og datafærdighed.

1.3.1. Enheder til at gemme og hente oplysninger

I løbet af de sidste units lærte du, hvordan du bruger computerværktøjer til at navigere online, mens du tager hensyn til din sikkerhed og privatliv. Vi dækkede også et meget vigtigt emne, som gør dig i stand til at være en ansvarlig digital borger, når du deler information, ved at evaluere datas sandhed.

Nu er det vores mål at tage dig gennem de tilgængelige værktøjer til at gemme dine oplysninger, gemme og hente dem, når du ønsker det.

På samme måde som du holder dit tøj organiseret i skuffer, har du mange ressourcer på din computer til at gemme information. Nedenfor præsenterer vi dig for nogle af dem.

Hukommelse og lagerenheder

ROM (Read Only Memory) is a type of permanent, internal memory that is used solely for reading.

RAM (Random Access Memory) is a working memory in which analysed data and programs are stored, while a computer runs. It allows reading and writing data, and is deleted/cleared when the computer shuts down.

CD (Compact Disc) is an optical disc used for data storage. The standard capacity of a CD is 700MB. CD-R is used for reading and writing data one time-only, while CD-RW for reading and writing data multiple times.

DVD (Digital Versatile Disc) is an optical disc which is, due to the larger capacity (about 4.7 GB), mostly used for video storage. Blu-ray disc (BD)- the successor to DVD, is an optical disk storage, it comes in different capacities, depending on how many layers it has and the capacity of each layer.

Memory card is a type of flash memory used to store data in digital cameras, cell phones, MP3 players etc.

USB Stick is a data storage device. It features small dimensions, relatively high capacity, reliability and speed. It belongs to the type of flash memory that remembers data, even when not under voltage i.e. they do not need electric power to maintain data integrity.

Figur 7 – identifikation og kort beskrivelse af hukommelses- og lagerenheder.

For at gemme information er der også en enhed kaldet intern harddisk, som er indlejret i computerens kabinet, og en ekstern harddisk, som er forbundet til en computer ved hjælp af et passende kabel eller USB-port, og som normalt bruges til at overføre data fra en computer til en anden eller til backup.

Når du downloader information fra internettet, er det vigtigt at huske, at vi bruger andres arbejde som artikler, bøger, billeder, videoer, kompositioner, videospil osv. Derfor skal vi forstå begreberne ophavsret, licensering og data beskyttelse. Men i den digitale æra har det været vanskeligt at etablere love om ophavsret vedrørende den information, der er lagt ud på nettet. For eksempel ejer sociale medier som Facebook ikke arbejde, der er lagt ud på deres hjemmeside, men du skal acceptere en licens, hvor Facebook må bruge dit arbejde til andre formål.

1.3.2. Ophavsret og databeskyttelse

ophavsret er en rettighed, som bruges til at beskytte ophavsmandens intellektuelle ejendom. Hvis nogen ønsker at bruge et sådant ophavsretligt beskyttet værk, skal de respektere de betingelser, hvorunder forfatteren som ejer har tilladt brugen af hans/hendes værk (betaling af gebyrer, henvisning til originalen osv.).

Persondatabeskyttelse

EU's charter om grundlæggende rettigheder fastslår, at EU-borgere har ret til beskyttelse af deres personoplysninger.

"Enhver har ret til beskyttelse af personoplysninger om ham eller hende" og til "adgang til data, der er indsamlet om ham eller hende, og ret til at få dem berigtiget"[9]

Europa-Kommissionen fremlagde sin EU-databeskyttelsesreform i januar 2012 for at gøre Europa egnet til den digitale tidsalder. Mere end 90 % af europæerne siger, at de ønsker de samme databeskyttelsesrettigheder i hele EU – og uanset hvor deres data behandles.

Direktiv 95/46/EF er referenceteksten på europæisk plan om beskyttelse af personoplysninger. Den opstiller en lovgivningsramme, der søger at finde en balance mellem et højt niveau af beskyttelse af privatlivets fred for enkeltpersoner og den frie udveksling af personoplysninger inden for Den Europæiske Union (EU). For at gøre dette sætter direktivet strenge grænser for indsamling og brug af personoplysninger og kræver, at hver medlemsstat opretter et uafhængigt nationalt organ med ansvar for beskyttelsen af disse data. Direktivet har til formål at beskytte personers rettigheder og friheder med hensyn til behandling af personoplysninger ved at fastlægge retningslinjer for, hvornår denne behandling er lovlig. Retningslinjerne vedrører:

[9] Kilde: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en

The quality of the data

- personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes. They must also be accurate and, where necessary, kept up to date

The legitimacy of data processing

- personal data may be processed only if the data subject has unambiguously given his/her consent or processing is necessary

Special categories of processing

- it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life. This provision comes with certain qualifications concerning, for example, cases where processing is necessary to protect the vital interests of the data subject or for the purposes of preventive medicine and medical diagnosis

Information to be given to the data subject

- the controller must provide the data subject from whom data are collected with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data etc.)

The data subject's right of access to data

Every data subject should have the right to obtain from the controller:

1. confirmation as to whether or not data relating to him/her are being processed and communication of the data undergoing processing;
2. the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive in particular, either because of the incomplete or inaccurate nature of the data, and the notification of these changes to third parties to whom the data have been disclosed.

Exemptions and restrictions

- the scope of the principles relating to the quality of the data, information to be given to the data subject, right of access and the publicising of processing may be restricted in order to safeguard aspects such as national security, defence, public security or the prosecution of criminal offences.

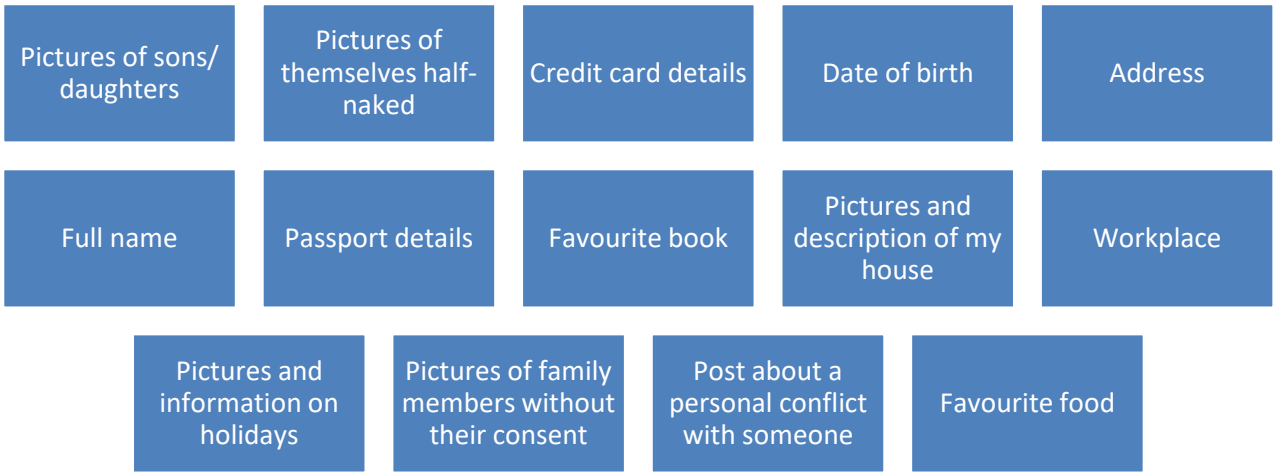
Figur 8 – Retningslinjer vedrørende beskyttelse af personoplysninger som fastsat i direktiv 95/46/EF.

1.3.3. Praktiske aktiviteter

Trin 1: Send hatten

Alle sidder i en rundkreds. I midten af cirklen placerer træneren en skala fra 1 til 5. Det kan være et stykke papir med tallene skrevet eller 5 papirer med hver et tal. Derefter forklarer træner, at en hat vil passere rundt med sætninger. Sætningerne beskriver personlige oplysninger fra rigtige mennesker, der blev lagt ud på nettet. Hver person skal tage et stykke papir inde fra hatten, læse det op og placere det i nærheden af et tal fra 1 til 5, hvor 1 betyder "ikke et alvorligt problem" og 5 betyder "meget alvorligt problem".

Mulige situationer:



Figur 9 – Identifikation af mulige situationer, der skal tages i betragtning i denne aktivitet.

Dette er blot nogle få eksempler, du kan bruge til at starte en samtale omkring personlige oplysninger, som alle deler online, nogle gange uden at tænke over det.

I slutningen af aktiviteten, når alle sætningerne er under tallene 1 til 5, ville det være interessant at diskutere, hvordan folk bedømte hver af dem. Hvorfor er det for eksempel ikke så alvorligt at dele en yndlingsmad som at dele billeder af familiemedlemmer uden deres samtykke?

Trin 2: Walking brainstorming

Denne aktivitet er en introduktion til emnet ophavsret, licensering og databeskyttelsesregler. Træneren sætter tre flipover-papirer op på væggen (vi foreslår, at du klæber papirerne med blu-tack) og navngiver dem med "copyrighting", "licensing" og "data protection".

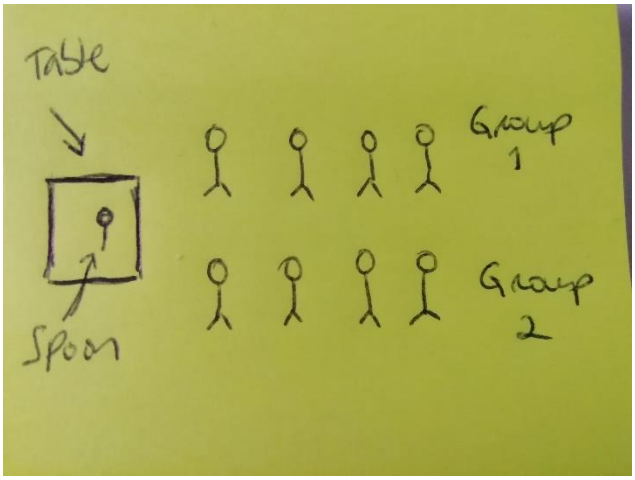
Eleverne får markører i forskellige farver, og de skal gå rundt i lokalet og skrive et ord eller flere i hvert papir, alt efter hvad der kommer til at tænke på, når de tænker på hvert emne. Det er vigtigt at fremhæve, at der ikke er rigtige/forkerte svar.

Når alle har skrevet mindst ét ord, kan du starte en diskussion og derefter præsentere information om emnerne. Du kan tilpasse denne aktivitet til et online format ved at bruge kollaborative læringsplatforme. Vi foreslår LAMS (Learning Activities Management System), som er en gratis og open source til at udvikle den slags aktiviteter online.

Trin 3: Test din viden

Denne aktivitet bygger videre på den viden, eleverne har erhvervet efter præsentationen af emnerne i denne enhed.

Træner instruerer klassen i, at de vil have 30 min til at gennemgå alt, hvad der er blevet undervist i enheden. Når tiden er gået, deles klassen op i to grupper. Træneren placerer en ske på et bord, og de to grupper placerer sig i to rækker med front mod hinanden i bordets retning (se figur 10).



Figur 10 – Inddeling af elever i to grupper.

- De to elever, der er tættest på bordet (de skal være på samme afstand) vil være ansvarlige for at plukke skeen, når de hører en alarm (træneren giver en lyd). Holdet, der først vælger skeen, har ret til at besvare et spørgsmål.
- Undervisere skal forberede et sæt spørgsmål vedrørende de underviste fag.
- Hvert rigtigt svar giver 1 point.
- Hvert forkert svar får -1 point.
- Tid til svar er 1 minut (træner kan øge den).
- I hver runde bytter holdet det medlem, der vælger skeen, så alle har mulighed for at gøre det. Hvis du kører denne aktivitet online, skal du muligvis tilpasse den til en slags "hvem vil være millionær?" spil.

Tillykke, du har nu gennemført modul 1.

Glem ikke at tjekke bilagene for yderligere ressourcer og dokumenter til støtte for selvstudium!

Modul 2: Kommunikation og samarbejde

Det andet modul indeholder information om samarbejdsplatforme og beskriver emner relateret til kommunikation og interaktion online.

Bemærk venligst, at praktiske aktiviteter beskrevet i hver enhed kan indebære støtte fra en erfaren træner. Selvom oplysningerne i manualen er skrevet på en måde, der er let at forstå, kan nogle handlinger, der støder op til de præsenterede oplysninger, kræve støtte fra erfarne personer.

Modul 2	**Meddelelse**					
Varighed	25 timer					
Mål	• At kunne bruge online teknologier til at samarbejde med andre mennesker, såsom udveksling af data og information eller organisering af arbejde i teams. • At kunne opføre sig hensigtsmæssigt i onlinemiljøet. • At være opmærksom på risici og fordele ved at have en online identitet.					
Enheder	2.1 Interaktion gennem digitale teknologier	2.2 Deling gennem digitale teknologier	2.3 Engagere sig i medborgerskab gennem digitale teknologier	2.4 Samarbejde gennem digitale teknologier	2.5 Netiquette	2.6 Håndtering af digital identitet

Træningsorganisation [10]	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring
Varighed	4 timer	4 timer	5 timer	3 timer	5 timer	4 timer

Bord 9 - Global struktur af Modul 2 – Kommunikation og samarbejde.

[10]Det kan være: Ansigt til ansigt, E-læring. Blended learning eller selvstudium.

2.1. Interagere gennem digitale teknologier

Enhed 2.1	Interagere gennem digitale teknologier
Varighed	4 timer
Mål	Grundlæggende kommunikation (hvordan man kommunikerer bedre) Eleverne vil overveje vigtigheden af e-mail, internetsøgning og digitale dokumenter Eleverne vil bruge digitale værktøjer til hverdagens opgaver på forskellige platforme Eleverne vil blive fortrolige med sociale medier
Indhold	2.1.1 Processen med kommunikation og kommunikationsstile 2.1.2 Effektiv e-mail-kommunikation 2.1.3 Social Media Training for begyndere 2.1.4 Praktiske aktiviteter
Ressourcer	Projektor til Powerpoint-præsentation (download præsentation fra hjemmesiden) Mobile enheder/ Computerstationer/tablets Hovedtelefoner Eksempel projekter
Træningsmetoder	Præsentation af træner Gruppeøvelse Diskussion / Debat Arbejde i par/små grupper Præsentation af deltagere Medievalg Projektbaseret læring (PBL) Flipped Classroom

Bord 10- Kompetenceenhedens opbygning 2.1. – Interagere gennem digitale teknologier i Modul 2 – Kommunikation og samarbejde.

2.1.1 Processen med kommunikation og kommunikationsstile

Grundlæggende kommunikation

Digitale kanaler og medier

En digital KANAL kan defineres som en grænseflade forbundet til world wide web, hvorigennem kommunikation kan foretages.

- På nettet – hjemmesider
- Til søgning - Søgemaskineresultater
- Kommunikation – E-mail- og beskedapps
- Online arrangementer – webinar
- Digitale medier - Videostreaming og musiksider
- Spil – Virtuelle spil

Et digitalt MEDIUM er en fysisk måde at gemme medier eller arkivere det på og kan opbevare

- Data
- Grafik
- Lyd og video

Digitale medier er velkendte som digitale medier, altså den form for medier, der kan skabes, ses, ændres og distribueres af elektroniske enheder.

Kommunikationsstile

- **Passiv:**Passive kommunikatører handler ofte ligegyldigt og undlader at udtrykke deres følelser eller behov, så andre kan udtrykke sig.

"Det betyder egentlig ikke så meget."

- **Aggressiv:**Aggressive kommunikatører udtrykker sig ofte på en "højlydt" måde og har en tendens til at udstede kommandoer, stille spørgsmål på en uhøflig måde og undlade at lytte til andre.

"Jeg har ret, og du tager fejl."

- **Passivt agressiv:**Disse kommunikatører kommunikerer højst sandsynligt med kropssprog og ser ud til at være bevidste om deres behov, men til tider kæmper de for at give udtryk for dem.

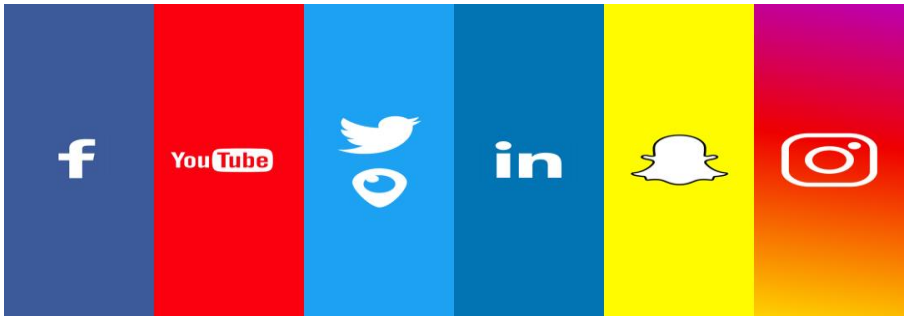
"Det er fint med mig, men bliv ikke overrasket, hvis en anden bliver sur."

- **Selvsikker:**Assertive kommunikatører kan udtrykke deres egne behov, ønsker, ideer og følelser, mens de også tager hensyn til andres behov.

"Jeg respekterer andres rettigheder."

Sociale medier

Sociale medier refererer til midlerne til interaktion mellem mennesker, hvor de skaber, deler og udveksler information og ideer i virtuelle fællesskaber og netværk. De bedste sociale medier apps Facebook, Instagram, Twitter, LinkedIn, YouTube.


YouTube
in

Praktiske aktiviteter

modul	2
Enhed	2.1
Varighed	3-4 timer
Type aktivitet	Praktisk aktivitet
Mål	Ved afslutningen af aktiviteten vil eleverne være i stand til at: ♦ Kommuniker og interager bedre gennem digitale værktøjer ♦ Brug af online platforme afhængigt af modtageren og det indhold, brugeren ønsker at kommunikere ♦ At forstå, hvordan man bruger alle digitale værktøjer og bliver fortrolig med sociale medier
Indstilling	For at udvikle denne aktivitet er det nødvendigt: ♦ En projektor ♦ Powerpoint slides (download fra hjemmesiden) ♦ Papir og kuglepenne ♦ Mobile enheder ♦ Computere ♦ En tavle ♦ Kridt
Debriefing aktivitet	I slutningen af aktiviteten skal eleverne tænke på: ♦ Hvad det vil sige at kommunikere og interagere gennem digitale teknologier. ♦ Hvilke fordele giver det? Hvilke ulemper? ♦ Hvordan har disse værktøjer ændret personlig kommunikation og gruppekommunikation i de seneste år?

Trin 1: 40-50 min

- Underviseren, efter at have lært alle elever at kende, starter med at introducere modulet i PowerPoint-slides, der giver en generel definition af, hvad der er kommunikation og interaktion, og hvad der defineres som digitale værktøjer.
- Underviseren vil tildele hver elev en partner og derefter til hvert par en computerstation.
- Underviseren vil bede hvert par elever om at vælge en app, såsom et ord til at skrive et kort brev eller et afsnit.
- Diskuter med eleverne, hvilken type kommunikation eller hvilken interaktion der er et brev.

Trin 2: 30-40 min

Underviseren vil gennem PowerPoint-slides introducere Fundamentals i kommunikationen.

Underviseren vil bede alle elever om det brev eller afsnit, de skrev for at identificere, hvem der er

a. Afsenderen
b. Modtageren
c. Beskeden
d. Koden

Debriefing aktivitet

- Underviseren vil diskutere med alle elever og spørge dem, hvad de betragter som kommunikationskanaler, og bede dem om at give nogle eksempler
- Underviseren vil liste alle eksempler på kommunikationskanaler og medier leveret af eleverne på tavlen.
- Underviseren vil præsentere kommunikationskanaler og medier gennem PowerPoint-dias
- Underviseren vil spørge, hvordan de ville kategorisere kanalerne, formelle, uformelle, uofficielle.

Trin 3: 60 min

Denne aktivitet er mere praktisk end de to første aktiviteter, men den vil også kombinere noget teori, da underviseren vil introducere de digitale værktøjer og vil lægge vægt på brugen af en online konto

- Underviseren vil introducere begrebet brugernavn, adgangskode og onlinekonto
- Underviseren vil guide eleverne til google.com på deres computerstationer for at oprette deres onlinekonto
- Eleverne gennem denne aktivitet vil arbejde i par, og hvert par deler en konto
- Når eleverne har oprettet deres Google-konto, vil underviseren guide og vise dem til Gmail og forklare formatet og layoutet af dette værktøj
- Bed eleverne om at skrive et lille bogstav eller et lille afsnit i det nye beskedvindue

Debriefing aktivitet

Underviseren vil foreslå nogle debriefingsspørgsmål

- Hvem ville du sende en mail til? Hvilken tone ville de bruge og hvorfor?
- Hvilken type kommunikation er e-mail bedst til?
- Hvilken slags medier eller filer kan man vedhæfte til en e-mail?

Trin 4: 30-40 min

- Underviseren baseret på den tidligere debriefing-aktivitet vil gennem PowerPoint-slides præsentere kommunikationsstile og kommunikationsstile, der bruges gennem digitale værktøjer
- Underviseren vil introducere og navngive alle sociale medier
- Underviseren vil guide eleverne trin for trin til at oprette en Facebook-konto ved hjælp af deres Gmail-e-mailadresse og logge ind
- Underviseren vil guide eleverne til at tjekke alle funktioner på Facebook og sende øjeblikkelige beskeder til de andre kolleger.
- Underviseren vil også guide dem trin for trin i at lave et lille indlæg

2.2. Deling gennem digitale teknologier

Enhed 2.2	Deling gennem digitale teknologier
Varighed	4 timer
Mål	Forbindelse med andre gennem digitale værktøjer Opsætning af delte mapper på en bestemt platform Brug og redigering af en delt fil
Indhold	2.2.1 Brug online konto på en digital platform 2.2.2 Konfigurer en delt fil på en platform 2.2.3 Brug kommentarer eller foretag justeringer på en delt fil 2.2.4 Praktiske aktiviteter
Ressourcer[11]	Computerstationer / tablets med internetadgang Power point-præsentation (download fra hjemmesiden) PowerPoint projektor Hovedtelefoner
Træningsmetoder	Præsentation af træner Gruppeøvelse Diskussion / Debat Arbejde i par/små grupper Medievalg Projektbaseret læring (PBL) Stationslæring

Bord 11- Kompetenceenhedens opbygning 2.2. – Deling gennem digitale teknologier af Modul 2 – Kommunikation og samarbejde.

Deling gennem digitale teknologier

Digitale teknologier er værktøjer, systemer, enheder og ressourcer, der genererer, lagrer eller behandler data. Nogle af de mest almindelige digitale teknologier omfatter sociale medier, onlinespil, multimedier og mobile enheder.

Hvad er deling med digitale teknologier?

[11] Materialer og udstyr.

Ifølge Digital Competence Framework 2.0 betyder det at dele data, information og digitalt indhold med andre gennem passende digitale teknologier som nævnt ovenfor.

Digitale værktøjer

- **Programmer**: Ord, Maling, Noter
- **Websites:** Google.com (Google drev)
- **Online kilder:**Podcasts, videoer, sociale medier

Lad os se, hvordan nogen kan dele en fil på Google Drev...

Hvad er Google Drev?
Google Drev er en fillagringsplacering udviklet af Google. Det er en internetbaseret tjeneste, der er tilgængelig som en hjemmeside og en app og gør det muligt at gemme filer i "skyen" og synkronisere filer på tværs af enheder.
Lad os nu tjekke det ud!!

1. Gå til drive.google.com på din computerstation
2. Log ind med dit Google-brugernavn og -adgangskode
3. Upload den fil, vi oprettede tidligere på Google Drev
4. Klik på den uploadede fil, og klik på del
5. Indtast din kollegas e-mailadresse under "Personer".
6. Klik send

Praktiske aktiviteter

modul	2
Enhed	2.2
Varighed	2 – 3 timer
Type aktivitet	Praktisk aktivitet
Mål	Ved afslutningen af aktiviteten vil eleverne være i stand til: ♦ Forbindelse med andre gennem digitale værktøjer ♦ Opsætning af delte mapper på en bestemt platform ♦ Brug og redigering af en delt fil
Indstilling[12]	For at udvikle denne aktivitet er det nødvendigt: ♦ En projektor ♦ Powerpoint slides (download præsentation fra hjemmesiden) ♦ Papir og kuglepenne ♦ Mobile enheder ♦ Computere
Debriefing aktivitet	I slutningen af aktiviteten skal eleverne tænke på: ♦ Hvad det vil sige at dele gennem digitale teknologier. ♦ Hvilke fordele giver det? Hvilke ulemper? ♦ Hvordan har disse værktøjer ændret informationsdeling i de seneste år?

Trin 1: 10 min

Underviseren vil introducere eleverne til begrebet deling og vil også give dem definitionen.

[12]Identificer venligst udstyr, materialer, dokumenter og eventuel support, der er nødvendig for at udføre denne aktivitet. Hvis du opretter et støttedokument, kan du også tilføje det her.

Debriefing aktivitet

Underviseren vil foreslå nogle debriefingsspørgsmål:

- Hvilken type information deler du normalt?
- Hvordan deler du disse oplysninger?
- Hvilke digitale værktøjer eller platforme kan bruges til at dele disse oplysninger?

Trin 2: 30-40 min

- Underviseren vil gennem PowerPoint-dias introducere simple digitale værktøjer såsom Word, Notes eller Paint til at skabe indhold
- Underviseren vil bede eleverne på hver af deres computerstationer om at vælge en af de demonstrerede apps til at skabe specifikt indhold, enten ordbaseret eller billedbaseret.
- Når alle elever har oprettet deres filer, vil underviseren bede dem om at gemme lokalt på deres computerstation.
- Underviseren vil præsentere de mest almindelige platforme til at dele indhold, Facebook, Instagram, mail, YouTube, Google Drev, Dropbox

Trin 3: 20 min

- Underviseren vil bede eleverne om at åbne et specifikt digitalt værktøj såsom Dropbox og guide dem trin for trin for at finde den fil, de har oprettet før og dele gennem Dropbox med resten af eleverne
- Underviseren vil derefter bede eleverne om at åbne en social medie-app såsom Facebook og vil bede eleverne om at dele deres oprettede fil som et opslag

Trin 4: 10-20 min

- Underviseren vil gennem slides præsentere enkle trin til, hvordan man redigerer en delt fil på Dropbox.
- Underviseren vil derefter bede eleverne om at redigere alle filer, der blev delt i den fælles mappe på Dropbox-platformen

2.3. Engagere sig i medborgerskab gennem digitale teknologier

Denne enhed vil introducere dig til to hovedkoncepter:

- Digitalt medborgerskab
- Cybersikkerhedsbevidsthed

Vi vil fokusere på at forstå, hvordan man identificerer cybersikkerhedsrisici, hvordan man forebygger dem og løser dem.

Enhed 2.3	**Engagere sig i medborgerskab gennem digitale teknologier**
Varighed	5 timer
Mål	- Forstå konceptet Digital Citizenship samt Cyber Security Awareness - Identificer cybersikkerhedsrisici - Sådan forhindrer du cyberangreb
Indhold	2.3.1 Digitalt medborgerskab 2.3.2 Grundlæggende begreber 2.3.3 Sikkerhed og privatliv 2.3.4 Praktiske aktiviteter
Ressourcer	Computerstationer og mobile enheder med internetadgang Hovedtelefoner Powerpoint projektor Power point-præsentation (download fra hjemmesiden) Sort tavle
Træningsmetoder	- Præsentation af træner - Gruppeøvelse Diskussion / Debat - Simulering / Rollespil - Medievalg - Projektbaseret læring (PBL) - Kooperativ læring - Flipped Classroom

Bord 12- Kompetenceenhedens opbygning 2.2. – Engagere sig i medborgerskab gennem digitale teknologier i modul 2 – Kommunikation og samarbejde.

2.3.1 Digitalt medborgerskab

Digitalt medborgerskab refererer til den adfærd, det positive engagement individer pålægger, når de træder ind i den digitale verden. Mere detaljeret er en Digital Citizen en person, der har viden og færdigheder til effektivt at bruge digitale teknologier til at kommunikere med andre, deltage i samfundet og skabe og forbruge indhold gennem digitale værktøjer.

2.3.2 Grundlæggende begreber

E-sikkerhed

Dette koncept er blevet et grundlæggende emne i den digitale verden og omfatter en persons viden om internetprivatliv og hvordan en persons adfærd kan bidrage til en sund interaktion med brugen af internettet. Almindelige farer: Phishing, malware, cybermobning, adgang til og udstationering af private oplysninger.

Omdømme

Moving along from the Age of Information to the Age of Reputation

Our digital reputation is how we are perceived online and is shaped and figured by the way an individual presents him/her self and the information other individuals post about them.

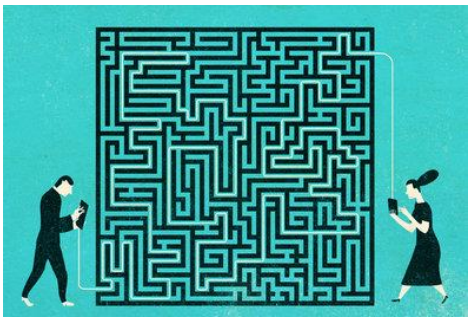
Digital Reputation is a concept that has shaped in such a way that has become more permanent than ever before since we as individuals have placed more trust in search results than any other source.

Relationer

Digitale relationer involverer at bruge teknologier til at udvikle en mere interaktiv og relevant interaktion mellem individer.

Disse teknologier kan bidrage både positivt og negativt specifikt i personlige relationer afhængigt af hvordan individer bruger teknologi og kan skabe problemer mellem partnere, hvilket potentielt kan skabe konflikt og utilfredshed i forholdet.

ELL



Etik

Digital Etik er studiet af, hvordan man kan håndtere sig selv etisk professionelt og på en måde via online og digitale medier.

Nogle eksempler på en etisk adfærd er, når en person:

1. Beder om tilladelse til at indsamle og opbevare data om brugere
2. Beder om tilladelse til at sælge eventuelle personlige data, der er blevet gemt
3. Har fået ret til at anmode om, at data om dem slettes.
4. Har fået adgang til persondata, der er blevet indsamlet og opbevaret

Digitale fodspor

Digitale fodspor eller digitale spor er registreringer af, hvad en person søger, besøger, skaber, deler, poster, installerer gennem digitale værktøjer på en mobilenhed eller på en computerstation.

En god Borger

- Fortaler for lige menneskerettigheder
- Behandler andre med respekt
- Stjæler eller beskadiger ikke andres ejendom
- Kommunikerer tydeligt respektfuldt og med empati
- Taler ærligt og gentager ikke udokumenterede rygter
- Beskytter sig selv og andre mod skade
- Projicerer et positivt selvbillede

En god digital borger

- Fortaler for lige digitale rettigheder for alle
- Søger at forstå alle perspektiver
- Respekterer digitalt privatliv, intellektuel ejendomsret og andre rettigheder for mennesker online
- Kommunikerer og handler med empati for andres menneskelighed via digitale kanaler
- Anvender kritisk tænkning til alle onlinekilder, inklusive falske nyheder
- Er opmærksom på fysisk, følelsesmæssig og mental sundhed, mens du bruger digitale værktøjer.
- Forstår varigheden af den digitale verden og styrer proaktivt digital identitet.

2.3.3 Sikkerhed og privatliv

Sikkerhed- Talrige processer, der beskytter en persons personlige oplysninger mod andre mennesker. Dette kan opnås på forskellige måder:

- VPN, virtuelle private netværk
- Antivirus programmer
- Stærke adgangskoder

Privatliv - En persons ret til at bevare og beskytte sin identitet og opretholde et trygt og beskyttet rum omkring ens integritet, fysiske tilstedeværelse, tanker, følelser og intime aktiviteter.

I den digitale verden skal privatlivets fred ses som en afgørende vigtig rettighed for individer som samfund og som et kollektiv.

2.3.4 Praktiske aktiviteter

modul	2
Enhed	2.3
Varighed	5 timer
Type aktivitet	Praktisk aktivitet
Mål	Ved afslutningen af aktiviteten vil eleverne være i stand til: ♦ Forstå konceptet Digital Citizenship samt Cyber Security Awareness ♦ Identificer cybersikkerhedsrisici ♦ Sådan forhindrer du cyberangreb
Indstilling[13]	For at udvikle denne aktivitet er det nødvendigt: ♦ Computerstationer og mobile enheder med internetadgang ♦ Hovedtelefoner ♦ Powerpoint projektor ♦ Sort tavle

[13]Identificer venligst udstyr, materialer, dokumenter og eventuel support, der er nødvendig for at udføre denne aktivitet. Hvis du opretter et støttedokument, kan du også tilføje det her.

Debriefing aktivitet	♦ Kridt I slutningen af aktiviteten skal eleverne tænke på: ♦ Hvordan folk interagerer online. ♦ Som online skal du være meget forsigtig med, hvordan du kommunikerer med andre. ♦ Sådan forhindrer du cyberangreb ♦ Sådan beskytter du en computerstation eller en mobilenhed, mens du surfer på internettet ♦ Sådan filtreres information på internettet og delt indhold

Trin 1: 30-40 min

- Underviseren vil have en dagsorden for at hjælpe med at holde lektionen på sporet og sikre, at eleverne ved og forstår, hvad de kan forvente under træningen
- Underviseren vil introducere modulet for alle elever gennem PowerPoint-slides og forklare konceptet Digitalt medborgerskab.
- Bed elever, der bruger deres stationer, om at se to problembaserede videoer, der fokuserer på, hvorfor digitalt medborgerskab er vigtigt.

Debriefing aktivitet

- Underviseren vil diskutere med eleverne, hvad de hidtil har forstået ved begrebet digitalt medborgerskab
- Underviseren vil også diskutere med eleverne de trusler og risici, man støder på, når man ikke søger på sikre websteder, og hvordan man håndterer sociale medier-relaterede problemer.

Trin 2: 60 min

- Underviseren vil introducere de grundlæggende begreber om Digitalt Medborgerskab
- Underviseren vil give eleverne eksempler og hjælpe dem med at blive internetalarm
- Underviseren vil opmuntre eleverne til at udveksle ideer mellem dem og demonstrere bevidsthed om farerne ved at levere case-scenarier
- Underviseren vil illustrere de to case-scenarier og diskutere nøglepunkterne i hvert scenarie
- Når de to scenarier er udarbejdet, vil underviseren derefter oprette et diagram med tre kolonner på tavlen med udtrykkene "Sikker", "Ansvarlig" og "Respektfuld" skrevet øverst i hver kolonne.
- Inviter eleverne til at give ord eller sætninger, der beskriver, hvordan folk kan handle sikkert, ansvarligt og respektfuldt online, og skriv dem i den relevante kolonne

- Få hver af eleverne til at bruge et stykke plastik og rive i stykker, forklare, hvad det vil forårsage for miljøet og knytte det til det digitale fodaftryk, når de ikke handler på en sikker, ansvarlig og respektfuld måde.

Trin 3: 50 min

- Underviseren vil introducere konceptet og definitionen af Digitalt spor og fodaftryk
- Underviseren vil give alle elever uddelingsark for at skrive ned, hvad de allerede ved, hvad de vil vide, og hvad de har lært
- Pædagogen vil bede to frivillige om at deltage i et rollespil
  Sig: "Forestil dig, at du går ned ad en overfyldt gade, og en fuldstændig fremmed kommer hen til dig og siger, at du lige har vundet en gratis rejse - alt du behøver at give ham er dit navn, alder, adresse, telefonnummer og adgangskoder til dit sociale netværk konti (Google+, Facebook osv.). Ville du tro ham?"

  Debriefing aktivitet
  Underviseren vil uddele en postvurdering, som vil blive diskuteret blandt eleverne

Trin 4: 45 min

- Underviseren vil begynde med at spørge, hvor vigtigt deres privatliv er for dem eller bedømme det fra 1 til 5 og registrere oplysninger på tavlen
- Underviseren vil derefter spørge eleverne, der siger, at det er uvæsentligt at have deres privatliv og opmuntre de andre elever til at debattere om emnet.
- Ved hjælp af nogle eksempler fra debatten diskuterer de med alle elever, hvad de forstår ved begrebet sikkerhed og privatliv
- Underviseren vil give definitionen af privatliv og sikkerhed og give eksempler på digitale værktøjer

Til sidst vil underviseren overstige det, der er blevet diskuteret i enheden, og forklare de rettigheder, alle har som digitale borgere, og spørge om sikkerheds- og privatlivsindstillingerne for deres sociale mediekonti på deres computerstationer.

2.4. Samarbejde gennem digitale teknologier

Enhed 2.4	Samarbejde gennem digitale teknologier
Varighed	3 timer
Mål	At lære eleverne at bruge digitale værktøjer til at samarbejde online med andre.
Indhold	2.4.1 Samarbejde gennem digitale teknologier – hovedkoncepter 2.4.2 Praktiske aktiviteter
Ressourcer	Tavle Stykker papir kuglepenne Krukke Computere
Træningsmetoder	Præsentation af træner Gruppeøvelse Diskussion / Debat Arbejde i par/små grupper Medievalg

Bord 13- Kompetenceenhedens opbygning 2.5. – Samarbejde gennem digitale teknologier i Modul 2 – Kommunikation og samarbejde.

2.4.1 Samarbejde gennem digitale teknologier – hovedkoncepter

Formålet med denne enhed er at lære eleverne, hvad det vil sige at samarbejde gennem digitale teknologier, at kende de mest almindelige værktøjer til at samarbejde online og at kunne identificere det rigtige værktøj til et bestemt behov.

Definition af samarbejde gennem digitale teknologier:

Ifølge definitionen i Digital Kompetence Framework 2.0 betyder samarbejde gennem digitale teknologier: "at bruge digitale værktøjer og teknologier til samarbejdsprocesser og til samkonstruktion og samskabelse af ressourcer og viden".

Hvorfor er samarbejde gennem digitale teknologier så vigtigt?

I dag er vi mere og mere vant til at bruge digitale teknologier i vores privatliv og arbejdsliv til at interagere med andre.

Udveksling af dokumenter, billeder, information eller brug af online-miljøet til at organisere arbejde eller studier er blevet stadig vigtigere, især siden Covid 19-pandemien tvang os til at bo, arbejde og studere derhjemme. Der er en række værktøjer, der gør det muligt for os at udveksle information i online-miljøet, på en hurtig og nem måde.

Især i et arbejdsmiljø er det blevet essentielt at kunne interagere med kolleger eller andre mennesker online, udveksle dokumenter og informationer og at kunne styre opgaver, organisere møder osv. Digitale værktøjer vil hjælpe os med at styre arbejdet (ikke kun eksternt)), fremskynde udvekslingen af information og øge teamets produktivitet.

Hvad er de mest nyttige værktøjer til at samarbejde i et online miljø?

Som allerede nævnt er der mange værktøjer, der hjælper os til at samarbejde online med andre. Nedenfor vil vi gerne dele og anbefale nogle af dem:

Skype; GoToMeeting; Zoom møder; Google Meet; Microsoft Teams: Alle disse værktøjer er webkonference- og onlinemødeværktøjer, der giver folk mulighed for at organisere møder eksternt eller nemt se hinanden, når folk er langt væk. Du kan også dele din skærm og vise præsentationer og filer til andre deltagere.

Google Drev; Dropbox: Med disse apps kan du gemme filer og gemme dem på et onlinerum, adskilt fra dine enheder. Dette er nyttigt, fordi du kan gendanne filen, selvom dine enheder har nogle problemer, forudsat at du har arkiveret dem her. Takket være disse værktøjer vil du desuden være i stand til at arbejde og samarbejde med andre mennesker ved at have muligheden for at dele dit rum eller dine dokumenter med kolleger, venner eller familiemedlemmer eller hvem du vil.

Google Kalender; Teamup: Disse er apps designet som en dagsorden. De ligner en kalender, som du kan organisere og personliggøre. Brugerfladen er meget enkel i begge, og du kan vælge at vise en enkelt dag, en uge eller endda længere tidsintervaller. Du kan markere dine aftaler, planlægge et møde og endda dele dem med andre mennesker.

Trello; Redbooth; Asana: Disse er projektstyringsværktøjer, der hjælper i arbejdsaktiviteter. Du kan oprette lister, tildele opgaver til andre medlemmer af dit team, der deler den samme plads, sætte deadlines og tilpasse alt så effektivt som muligt.

Google Form: Google-applikationen giver dig mulighed for at oprette undersøgelser frit og meget nemt. Du kan tilpasse dine undersøgelser og bruge forskellige måder at stille spørgsmål på: flere svar, åbne svar, tilfredshedsscore osv.

2.4.2 Praktiske aktiviteter

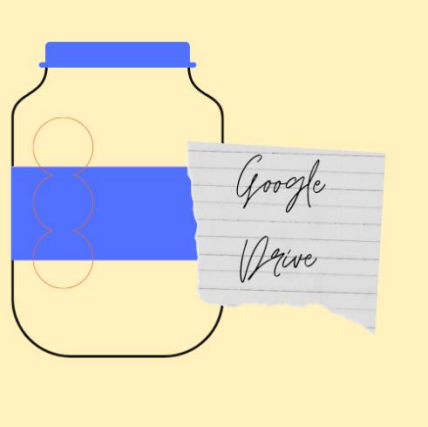
Trin 1: Krukken med værktøjer

Underviseren opregner flere værktøjer, som kunne foreslås til eleverne.

Alle de værktøjer, vi foreslår, er digitale open source-værktøjer. Pædagogen kan indsætte så mange værktøjer, han/hun vil (mindst ét pr. elev).

Vi foreslår følgende: Google Drev, Trello, Dropbox, Google Kalender Google Form osv.).

Pædagogen skriver navnet på værktøjet på et stykke papir og lægger det i krukken.



På dette tidspunkt er det elevernes tur: En ad gangen tager eleverne et stykke papir i krukken og siger højt navnet på det værktøj, de har fundet.

Underviseren stiller nogle spørgsmål til eleven og klassen:

- Hvad bruges dette værktøj til?
- Har du nogensinde brugt dette værktøj?
- Ved du, hvordan det virker?
- Kender du andre værktøjer, der fungerer på samme måde?
- Tror du, at dette værktøj er nyttigt til at fremme samarbejde?

Underviseren vil lede diskussionen, men vil forsøge at stimulere samtalen blandt eleverne.

Når alle noterne i krukken er færdige, vil underviseren skrive alle navnene på de værktøjer, der er kommet ud, ned på en tavle og forklare bedre for eleverne, hvordan de arbejder.

Ved afslutningen af aktiviteten vil underviseren foreslå nogle debriefingsspørgsmål:

- Ved du, hvad det vil sige at samarbejde gennem digitale teknologier?
- Hvordan kan de værktøjer, vi har set, hjælpe folk med at samarbejde hurtigere og nemmere?

Trin 2: Lad os prøve det!

Denne aktivitet er mere praktisk end den første og tjener til at omsætte den mere teoretiske viden, der er erhvervet under den første del, i praksis.

Eleverne arbejder i par.

Underviseren tildeler dem et værktøj, der skal testes blandt dem, der er nævnt i den første aktivitet.

På dette tidspunkt, afhængigt af værktøjet "modtaget", vil underviseren bede eleverne om at udføre små opgaver.

Opgaverne kan være mange og forskellige, og det afhænger af de værktøjer, pædagogen beslutter sig for at præsentere for sine elever.

Oprette en delt mappe, sende en tung fil, oprette et onlinemøde og invitere nogle kontakter osv.

Eleverne vil prøve et værktøj i 30 minutter, og de kan rotere med andre for at give alle mulighed for at prøve så mange værktøjer som muligt.

Ved afslutningen af aktiviteten vil underviseren foreslå nogle debriefingsspørgsmål:

- Fandt du de værktøjer, du prøvede, nyttige?
- Kendte du dem allerede?
- Tror du, de er nyttige i arbejdssammenhæng og videre?
- Hvad ville du bruge dem til?

2.5. Netiquette

Enhed 2.5	Netiquette
Varighed	5 timer
Mål	At lære eleverne den korrekte adfærd, der bør opbevares i et online miljø.
Indhold	2.5.1 Hvad betyder det Netiquette? 2.5.2 Praktiske aktiviteter
Ressourcer	En tavle; Kridt; Post-it; Papir og kuglepenne Casestudie 1 Casestudie 2
Træningsmetoder	Gruppeøvelse Diskussion / Debat Arbejde i par/små grupper

Bord 14- Kompetenceenhedens opbygning 2.6. – Netiquette af modul 2 – Kommunikation og samarbejde.

2.5.1 Hvad betyder det Netiquette?

Formålet med denne enhed er at lære eleverne at opretholde korrekt adfærd i onlinemiljøet. At respektere andre og de steder, hvor vi er, er lige så vigtigt i det fysiske miljø som i det online. Undervisning i disse emner er meget vigtigt, især fordi online-folk bliver mere aggressive eller slemme over for andre mennesker. Der er mange eksempler på fænomener forbundet med dårlig onlineadfærd, cybermobning, body-shaming er blot nogle få eksempler på adfærd, som vi dagligt er vidne til på nettet, for ikke at tale om episoder med racisme og had mod minoriteter generelt. Uddannelse til at respektere andre er afgørende for at forhindre en sådan adfærd.

Definition af Netiquette

Ifølge definitionen i Digital Competence Framework 2.0 betyder netiquette: ”At være opmærksom på adfærdsnormer og knowhow, mens du bruger digitale teknologier og interagerer i digitale miljøer. At tilpasse kommunikationsstrategier til det specifikke publikum og være opmærksom på kulturel og generationsmæssig mangfoldighed i digitale miljøer”.

Hvilken adfærd betragtes som et dårligt eksempel på netiquette?

Generelt kan vi betragte al den onlineadfærd, der er respektløs over for andre, som et dårligt eksempel på netiquette. Disse holdninger kan være af forskellig karakter.

Manglende respekt for intellektuel ejendom:deling af indhold, fotos, materialer af andre uden at citere kilden betragtes som forkert og et eksempel på dårlig netiquette (Ud over at antyde juridiske forpligtelser, som vi ikke vil diskutere her).

Vi bør altid tjekke, hvor vi får dette indhold, og se, om det er open source, eller om vi skal citere kilden, når vi bruger det.

Respekterer ikke andres meninger:ikke at respektere andre menneskers meninger og derfor indtage fjendtlige og fornærmende holdninger til disse mennesker er et eksempel på dårlig netiquette. Vi bør altid forsøge at etablere en dialog med andre uden at bruge ord eller toner, der er upassende, eller som kan støde andre.

At udtrykke os selv på en respektløs måde:Når vi skriver en besked, en e-mail eller et indlæg, skal vi være opmærksomme på, hvordan vi skriver, og hvordan vi udtrykker os selv og vores ideer. Husk altid, at folk på den anden side ikke ser vores udtryk eller hører vores tonefald, og det kan føre til misforståelser. Derfor er det vigtigt at være forsigtig, når du udtrykker dig online. Brug af tvetydigt eller fjendtligt sprog, brug af store bogstaver, ikke underskrift, ikke kontekstualisering af indholdet af din besked er blot nogle få eksempler på dårlig netiquette. Husk også at bruge formelt eller uformelt sprog afhængigt af den person, du har med at gøre, om det er en ven, en bekendt, en kollega eller en fremmed.

Manglende respekt for andres privatliv: Mange mennesker deler en masse billeder eller private oplysninger om sig selv på sociale netværk, men vær omhyggelig med altid at respektere andres privatliv og aldrig dele følsomme data uden den anden persons tilladelse.

2.5.2 Praktiske aktiviteter

Trin 1: Hvilken hører ikke til?

Underviseren skriver på en tavle forskellige online adfærd, der har at gøre med netikette, nogle positive eksempler og nogle negative eksempler.

I denne første aktivitet skal eleverne finde ud af, hvilke elementer der ikke har noget at gøre med de andre i en gruppe af gode og dårlige eksempler på netiquette.

Formålet med øvelsen er at identificere den dårlige adfærd inde i gode.

Kald én elev ad gangen til tavlen, og bed dem om at sætte en ring om dårlige eksempler på netiquette.

I sidste ende vil underviseren rette de svar, som eleverne har givet.

I slutningen af denne aktivitet inviterer underviseren eleverne til at reflektere over den adfærd, som folk holder online. Underviseren vil foreslå nogle debriefingsspørgsmål:

- Hvad er den adfærd, der gør dig utilpas online?
- I onlinemiljøet, har du nogensinde bemærket brugernes brug af dårlig opførsel?
- Har du nogensinde prøvet at forklare andre, hvad netiquette er?

Tips:

- Denne aktivitet kan også udføres ved hjælp af post-it sedler til at hænge på en væg.
- Denne aktivitet kan også udføres online ved hjælp af et værktøj såsom jamboard (https://jamboard.google.com/).

Trin 2: Tastaturkriger

Til denne øvelse foreslår underviseren eleverne forskellige tekster, hvor folk interagerer med hinanden online (f.eks. chat, e-mail, ofte stillede spørgsmål, kommentarer osv.).

To casestudier kan bruges i denne aktivitet.

Casestudie 1

En e-mail-udveksling mellem to kolleger

Anna og Elisabeth er to kollegaer, der arbejder i samme virksomhed. Anna arbejder i den administrative salgsafdeling, mens Elizabeth styrer forholdet til kunden og tilrettelæggelsen af arrangementer. Elisabetta bestilte nogle flyers og plakater for at offentliggøre begivenheden, men der var forsinkelser i leveringen.

Objekt: Sommerfestival_leveringsforsinkelser

Anna:

Kære Elizabeth, jeg skriver til dig med henvisning til bestillingen af flyers og plakater til den sommerfest, du bad om. På grund af Covid 19-pandemien har vores trykkeri desværre informeret os om, at der vil være en forsinkelse i leveringen.

Jeg giver dig besked, så snart vi har modtaget materialerne.

Med venlig hilsen

Anna

Elizabeth:

Hej Anna. Jeg forstår, at Covid har givet mange problemer, men det er et meget alvorligt problem for festivalens tilrettelæggelse. Det er mig, der skal tale med klienten, hvad skal jeg fortælle ham?

HVORDAN FREMMER JEG BEGIVENHEDEN NU?

Kunden ønsker materialerne inden udgangen af ugen. INGEN UNDSKYLDNINGER.

SKIFT PRINTMAKER, hvis det er nødvendigt! FORSTÅR DU MIG?

Anna:

Kære Elizabeth,

Jeg beklager meget, at denne forsinkelse forårsager problemer med dit arbejde.

Vi har desværre allerede betalt for materialet på forhånd, og vi kan ikke få pengene tilbage på nuværende tidspunkt. Prøv at forklare situationen for din klient, jeg er sikker på, at han vil forstå.

Tillid til dit samarbejde,

Jeg ønsker dig en god dag.

Med venlig hilsen

Anna

Elizabeth:

Jeg vil prøve at forklare ham situationen og bede om mere tid, men jeg ønsker ikke at tage ansvar for dette problem, hvis det er nødvendigt, vil jeg give nummeret på servicedirektøren.

SÅDAN VIL JEG HÅNDTERE DETTE PROBLEM.

Elizabeth

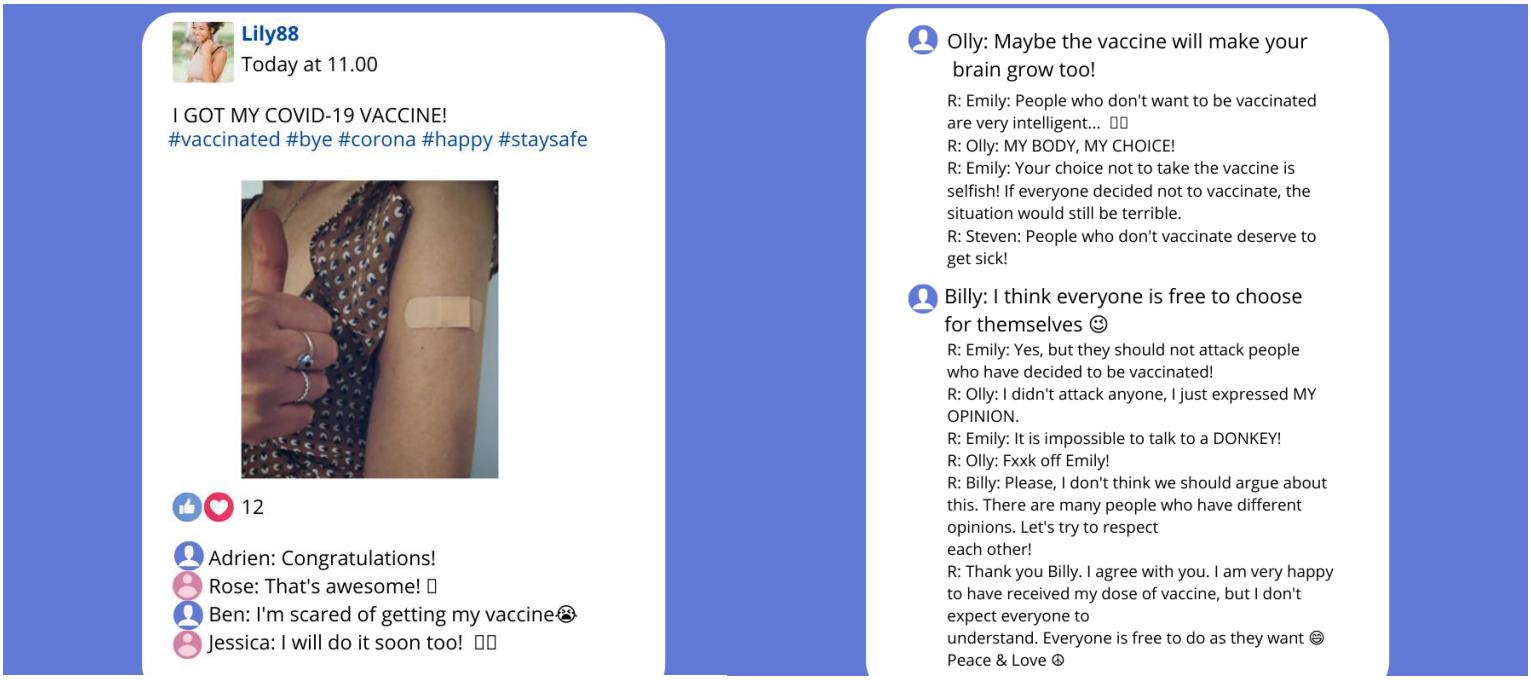
Underviseren inviterer eleverne til at reflektere over teksten:

- Hvordan fremstår Anna? Har hun en pæn holdning til Elisabeth eller ej?
- Og Elisabetta til Anna?
- Hvad er Elisabeths holdning til problemet? Er hun omfattende over for sin kollega eller ej?
- I teksten er der nogle eksempler på dårlig netiquette. Kan du finde ud af, hvad de er?

Efter at have besvaret underviserens spørgsmål, skal deltagerne forsøge at omskrive teksten og transformere adfærden fra negativ til positiv.

Casestudie 2

En pige (Lily) poster på sin Facebook-profil et billede efter at have modtaget sin første dosis af vaccinen mod Covid 19:



Underviseren inviterer eleverne til at reflektere over teksten:

- Hvad synes du er dårlig netiquette i disse kommentarer?
- Hvordan ville du have reageret på Ollys kommentar?
- Tror du, at Emily svarede ordentligt til Billy?
- Hvem synes du, har handlet korrekt i disse kommentarer?
- Kan du finde dårlige og gode eksempler på netiquette i teksten?
- Hvorfor tror du, det er nemmere at være ond online?
- Har du nogensinde været en tastaturkriger?

- Hvad gør du, når du erkender, at nogen bruger ond adfærd online?

Efter at have besvaret underviserens spørgsmål, skal deltagerne forsøge at omskrive teksten og transformere adfærden fra negativ til positiv.

Trin 3: Netikettemanifestet

I den sidste aktivitet går underviseren hen til tavlen og beder eleverne om at sammenskrive "Netiquette-manifestet", dvs. al den positive adfærd, som de mener bør holdes online.

Eleverne bør diskutere, hvad der er hovedreglerne, og derefter liste omkring ti eksempler på god netetikette.

Dette er klassens "Netiquette Manifesto", og alle skal forpligte sig til at respektere det.

Når manifestet er blevet besluttet, kan underviseren forklare eleverne en kort forklaring af netiquettens teori.

Ved slutningen af aktiviteten inviterer underviseren eleverne til nøje at reflektere over den måde, hvorpå folk skal interagere online, og hvordan eleverne gerne vil sprede og undervise andre i de regler, de har skrevet (ved at bruge sociale medier? Dele manifestet? osv.)

2.6. Håndtering af digital identitet

Enhed 2.6	Håndtering af digital identitet
Varighed	4 timer
Mål	At lære eleverne, hvad det vil sige at have en digital identitet, og hvordan de skal tage sig af den.
Indhold	2.6.1 Definitioner og beskyttelse af identitet 2.6.2 Praktiske aktiviteter
Ressourcer	Papir og kuglepenne Computere
Træningsmetoder	Gruppeøvelse Diskussion / Debat Arbejde i par/små grupper Simulering / Rollespil

Bord 15- Kompetenceenhedens opbygning 2.7. – Håndtering af digital identitet af Modul 2 – Kommunikation og samarbejde.

2.6.1 Definitioner og beskyttelse af identitet

Dette modul har til formål at gøre eleverne opmærksomme på al den information, vi efterlader online om os selv, og som repræsenterer vores digitale identitet. Digital identitet er noget, der relaterer til os, til vores person. For eksempel, når vi bruger et ID og en adgangskode til at autentificere os selv på en hjemmeside, bruger vi vores digitale identitet. I dag lever vi i en verden, hvor flere og flere tjenester kræver, at vi logger ind fra enheder, både private og offentlige. E-handel, bank, sundhedstjenester, skattetjenester er blot nogle få eksempler. Hver gang vi registrerer vores digitale identitet eller foretager visse handlinger online, bliver vores private data taget og registreret, ofte uden at brugeren selv er klar over det. Det er derfor, vi skal være opmærksomme og lære, hvordan vi bedst administrerer vores digitale identitet online.

Definition af håndtering af digital identitet

Ifølge definitionen i Digital Competence Framework 2.0 betyder håndtering af digital identitet: ”At skabe og administrere en eller flere digitale identiteter, at kunne beskytte sit eget omdømme, at håndtere de data, man producerer gennem flere digitale værktøjer, miljøer og tjenester”.

Hvorfor skal vi bekymre os om vores data?

Hver gang vi giver samtykke til privatlivets fred for at få adgang til et websted, downloade en app, besvare undersøgelser på sociale medier eller gå ind på et websted ved hjælp af vores oplysninger, genererer vi data. Disse data er relevante for mange virksomheder, fordi de afslører forbrugeradfærd. Vi giver ofte vores data væk eller giver samtykke til brugen af dem uden selv at være klar over det.

Men online efterlader vi ikke bare spor af, hvad vi kan lide og ikke kan lide som forbrugere, vi efterlader også meget vigtige private oplysninger, som hvis de bruges af andre, kan være meget skadelige for os. Tænk blot på vores kreditkortoplysninger eller vores sociale konti med billeder og personlige oplysninger.

Identitetstyveri

Når vores digitale identitet bliver hacket, og vores personlige eller økonomiske data bliver stjålet, kan vi tale om cyberkriminelle. De er folk, der specialiserer sig i online tyveri. De hacker ind i vores systemer eller bruger tricks til at få os til at tro, at de kan give os vores data på sikre websteder eller apps, mens de faktisk stjæler dem fra os.

Disse kriminelle efterligner dig og stjæler dine penge og information. For eksempel har nogle influencers (meget kendte personer på sociale medier) annonceret at få deres identitet stjålet af en hacker, som stjal deres sociale mediekonti og krævede en løsesum for at give dem tilbage.

Hvordan forsvarer vi os mod cyberkriminelle?

Først med bevidsthed. At vide, hvordan cyberkriminelle fungerer, og hvordan de kan stjæle din digitale identitet, er en nøglefaktor til at forhindre dem.

Så skal du være meget forsigtig. Åbn for eksempel aldrig mistænkelige e-mails eller beskeder, der når os. Ofte udgiver disse cyberkriminelle sig for at være organisationer, som vi har en service med (f.eks. en bank), så vi skal være i stand til at genkende, om de oplysninger, vi modtager, er sande eller ikke. er det skrevet korrekt på dit sprog? Er der nogle mærkelige tegn? Taler det om operationer, som du ikke kender til? Hvis du har den mindste mistanke, skal du ikke klikke, downloade eller røre ved noget. Er det for eksempel din bank, så ring til din filial og bed om en forklaring. Klik aldrig på mistænkelige links.

Dette fænomen kaldes phishing-angreb og er virkelig farligt for de personer, der er berørt af det.

Hvad er nogle måder at beskytte vores digitale identitet på?

- **Brug to-faktor-godkendelse:** Autentificering af din identitet sker ikke kun gennem ét trin (f.eks. adgangskode), men også gennem yderligere trin, såsom indtastning af en kode eller autorisation via telefonen.
- **Skift og diversificere adgangskoder:** Brug ikke de samme adgangskoder til alle dine konti, og prøv at ændre dem ofte.
- **Undgå at dele følsomme oplysninger**: vær forsigtig med den slags data, du deler, og prøv kun at dele det væsentlige online, såsom din hjemmeadresse (pas på geoplacering på billeder, du poster på sociale netværk!).

En digital borgers rettigheder

- Digitalt medborgerskab refererer ifølge Europarådet til evnen til at engagere sig positivt, kritisk og kompetent i det digitale miljø ved at trække på evnerne til effektiv kommunikation og skabelse, men det refererer også til den evne en borger anvender, når han deltager på en respektfuld måde over for menneskerettigheder og værdighed gennem ansvarlig brug af teknologi.
- En digital borger har ret til at nyde rettighederne til privatliv, sikkerhed, vurdering og inklusion og ytringsfrihed. Men som borger med disse rettigheder har den digitale borger visse forpligtelser såsom etik og empati og andre forpligtelser for at garantere et sikkert og ansvarligt digitalt miljø for alle digitale borgere.

2.6.2 Praktiske aktiviteter

Trin 1: Private eye-spillet

Forestil dig, at du taler med en veninde, der fortæller, at hun har mødt en klassekammerat fra gymnasiet.

Du er nysgerrig efter at vide mere om den person, som du var så tæt på, da du var teenager.

Prøv at samle hans for- og efternavn på internettet og udvid derefter forskningen (du kan også lave research på dig selv eller på en person, du kender).

- Hvad fandt du ud af om den person?
- Hvilke værktøjer har du brugt til at hjælpe dig i din forskning?
- Hvilke platforme konsulterede du?
- Prøv at besvare følgende spørgsmål:
    - Hvilken by bor han/hun i?
    - Er han/hun gift?
    - Hvad studerede han/hun?
    - Hvad er hans/hendes job?

Ved afslutningen af aktiviteten inviterer underviseren eleverne til nøje at reflektere over, hvilken information vi deler online.

Trin 2: Hvor sikker er din adgangskode?

I denne aktivitet ønsker underviseren at lære eleverne vigtigheden af at have en sikker adgangskode på deres konti.

Underviseren beder eleverne forestille sig at skulle forberede adgangskoder til en af følgende personer:

Helen Smith	Alejandro Garcia	María Ivanov
• Born: 25th June 1988 • Live in: Los Angeles (USA) • Married • She has got a dog named Oliver	• Born: 11th March 1965 • Live in: Madrid (Spain) • Single • He loves motorbikes	• Born: 1st December 1952 •Live in: Sofia (Bulgaria) • Married • She has three children

Figur 11 – Profiler, der skal overvejes for at forberede adgangskoder.

- **Prøv at skrive den forskellige adgangskode for hver person, der leger med ord (mindst 5). T**hint om en anden adgangskode afhængigt af den konto, du skal oprette den til (ei, bank; Facebook; privat e-mail; arbejds-e-mail, e-handel osv.).
- Test nu sikkerhedsniveauet for din adgangskode online (der er flere platforme, som du f.eks. kan bruge https://howsecureismypassword.net/).

Ved afslutningen af aktiviteten inviterer underviseren eleverne til nøje at reflektere over, hvordan man opretter en god adgangskode for at garantere et sikkerhedsniveau online.

Underviseren vil foreslå nogle debriefingsspørgsmål:

- Hvordan opretter du dine adgangskoder? Bruger du altid den samme til alle sider, eller har du forskellige?
- Tror du, at der er websteder, hvor du har brug for et højere niveau af adgangskodesikkerhed end andre?
- Hvilke tricks skal bruges til at skabe sikre online adgangskoder?
- Hvor ofte skal adgangskoder ændres?
- Ved du, hvordan identitetstyve kan stjæle dine adgangskoder?

Tillykke, du har nu gennemført modul 2.

Glem ikke at tjekke bilagene for yderligere ressourcer og dokumenter til støtte for selvstudium!

Modul 3: Indholdsskabelse

Modul 3 har fokus på Content Creation til den digitalt kompetente borger. Vi sigter mod at skabe en fælles forståelse af, hvad det vil sige at være en digitalt kompetent borger samt at udvikle og teste materialer, der skaber en klar vej til opkvalificering af dig selv inden for de vigtigste relevante digitale områder.

Inden for dette modul vil vi dække:

- Udvikling af digitalt indhold - At skabe og redigere digitalt indhold i forskellige formater, at udtrykke sig gennem digitale midler.

- Integration og re-udarbejdelse af digitalt indhold - At modificere, forfine, forbedre og integrere information og indhold i en eksisterende viden for at skabe nyt, originalt og relevant indhold og viden.

- Copyright og licenser- At forstå, hvordan ophavsret og licenser gælder for data, information og digitalt indhold

- Programmering - At planlægge og udvikle en sekvens af forståelige instruktioner til et computersystem for at løse et givet problem eller udføre en specifik opgave.

Vi vil skitsere, hvordan du kan skabe og redigere digitalt indhold for at forbedre og integrere dine oplysninger i et eksisterende materialemateriale, samtidig med at vi fremhæver de vigtige spørgsmål omkring ophavsret og licensering i den digitale sfære. Vi vil også kort berøre programmeringsaspekterne af, hvordan man bruger computersystemer.

Bemærk venligst, at praktiske aktiviteter beskrevet i hver enhed kan indebære støtte fra en erfaren træner. Selvom oplysningerne i manualen er skrevet på en måde, der er let at forstå, kan nogle handlinger, der støder op til de præsenterede oplysninger, kræve støtte fra erfarne personer.

Modul 3	Indholdsskabelse			
Varighed	10 timer			
Mål	For at forstå nuancerne og uddybe dine evner til at skabe indhold			
Enheder	3.1.Udvikling af digitalt indhold	3.2 Integrering og genudarbejdelse af digitalt indhold	3.3 Copyright og licenser	3.4 Programmering
Træningsorganisation	E-læring	E-læring	E-læring	E-læring
Varighed	2,5 timer	2,5 timer	2,5 timer	2.5 timer

Bord16 - Global struktur af Modul 3 – Indholdsskabelse.

Bemærk: Modul 3 praktiske aktiviteter præsenteres i Power Point slides, som du kan downloade fra ressourcesektionen på projektets hjemmeside.

3.1 Udvikling af digitalt indhold

Enhed 3.1	Udvikling af digitalt indhold
Varighed	2,5 timer
Mål	Øget viden om Mojo udstyr, praktiske måder at filme samt forståelse for positionering, lys og vinkler. Oversigt over Facebook live, Mobile apps til udvikling af digitalt indhold. Endelig et indblik i computerens redigeringsprogrammer til dit digitale indhold
Indhold	Autonome, fleksible ressourcer, der kan bruges på farten - E-Learning
Ressourcer	PC/mobil eller tablet til e-learning Power point-præsentation (download fra hjemmesiden)
Træningsmetoder	Præsentation af træner Flipped Classroom

Bord17 - Opbygning af kompetenceenheden 3.1.- Udvikling af digitalt indhold i Modul 3 – Indholdsskabelse.

3.1 Udvikling af digitalt indhold

5 typer digitalt indhold

Blogging

Blogindlæg er en grundlæggende måde at skabe engagerende indhold til dine brugere online! Ligesom den gammeldags avis elsker mange mennesker at sætte sig ned og nyde en velskrevet, indsigtsfuld blogindlæg eller artikel. Du kan dele masser af information i en ikke-formel indstilling, præsentere dig selv for dine læsere og skabe en forbindelse med dem og tilslutte dem for at komme tilbage efter mere! Det kan være tidskrævende at vedligeholde en succesfuld blog, så det anbefales, at du opretter en materialebank, før du sparker det hele i gang. Kom med nogle ideer til dine første 2-3 måneders blogindlægsindhold, samt implementering af en tidsplan for upload for at holde dine læsere engagerede, dette vil hjælpe dig til at være en regelmæssig og konsekvent plakat!

Inspireret til at starte din egen blog - find mere information her:

https://www.wix.com/blog/2021/02/how-to-start-a-blog/?utm_source=google&utm_medium=cpc&utm_campaign=9852964004^122617225367&experiment_id=^b^504114447774^^_DSA&gclid=CjwKCAjwh5qLBhALEiwAioods-cylXXhYEWcT_ZrqTbAeIxQDqSkTV_pdKfnoxlptSsbyl02Iw87MxoC6dwQAvD_BwE

Langformet indhold

I den øjeblikkelige verden, vi lever i i dag, kan langformat indhold være lidt af et gamble. De fleste mennesker kan lide at modtage deres information i korte og søde, mundrette bidder, men definitionen af langform tilpasser sig til at afspejle dette. Nogle mennesker definerer langt indhold som artikler, der er længere end 700 ord, mens andre mener, at det skal overstige 1800 ord. Disse typer artikler med langt indhold kan appellere til dine ivrige læsere, det engagerer dem og giver dem en flugt, som de længes efter.

Denne type indhold kan fungere særligt godt på grund af fokus på søgemaskineoptimering, herunder nøgleordsoptimering. Ved at udpege de ord, du bruger ofte, og som vil være af interesse for din målgruppe, kan du sikre, at dit indhold lander på deres skærm! Vær smart og kyndig med dit indhold, og dette kan fungere usædvanligt godt.

Tips til at gøre dit indhold læsbart og værdifuldt- https://medium.com/swlh/10-tips-to-make-long-form-content-readable-and-valuable-5b6e117965ae

Infografik

Iøjnefaldende, engagerende og let at skabe! Infografik er deroppe med det mest brugte digitale indhold i online-sfæren, grunden til dette er, at de fanger brugerens blik og trækker dem ind, der gerne vil vide mere. De kan være virkelig engagerende, give billeder af høj kvalitet, masser af information i et hurtigt øjebliksbillede. Derudover er de super nemme at lave!

Du kan bruge værktøjer såsom Canva eller endda Microsoft PowerPoint til at skabe smukke varemærkebilleder med korthed, som du kan dele med dit publikum. Vær ikke bange for at dele disse på dine sociale medier for mere effekt af begivenheden!

Klik her for at prøve Canva- https://www.canva.com/

Podcasts

I de seneste fem år er udbredelsen af podcasts tidoblet. Hvis du sidder ved frokostbordet i dag, spørg bare efter, hvem der lytter til podcast-indhold, og vi kan garantere, at du vil have mindst 50 % positiv feedbackrate! Podcasts er den nye og innovative måde at indtage information af enhver art. Fra ægte krimi, til komedie, til naturhistorie, hvis du har en mærkelig eller skør interesse, er chancerne for, at der allerede er en podcast, der dækker det i detaljer!

Denne type indhold giver folk mulighed for at absorbere digitalt indhold, selv mens de er på farten, for eksempel ude at løbe, eller mens du er på din morgenpendling, kan du nemt komme ind i en podcast, stadig koncentrere dig om opgaven med en nyttig dosis af underholdning eller uddannelse.

Klik her for at se, hvordan du kommer i gang med din podcast - https://www.thepodcasthost.com/planning/how-to-start-a-podcast/

Endelig video!

Video er KONGE af digitalt indhold, i nutidens visuelle samfund er video den ideelle måde at komme i kontakt med dit publikum på på en måde, der vil gøre en enorm indflydelse! Det anslås, at YouTube har over 2 milliarder aktive brugere MÅNEDLIG. Hvis du vil vælge et digitalt indhold for at bruge din tid og dine ressourcer på at lade det være videooprettelse. Videoindhold er meget forskelligartet, tilpasningsdygtigt og kan være fængslende for brugeren, vi kender alle følelsen af at scrolle gennem sociale medier forbi lange indlæg, billeder og få øjet fanget af en smukt udformet video med fordybende billeder, musik og beskeder.

Videomarketing er en øjeblikkelig publikumsbehag, YouTube genererede $19,7 milliarder i omsætning i januar 2021.[14]Og TikTok har overtaget fra Facebook, Instagram og Snapchat som den mest populære sociale medieplatform. Korte introduktions- eller forklaringsvideoer kan være meget mere effektive til at engagere dine brugere, idet de optager lidt af deres tid, men efterlader dem med masser af information til gengæld!

Inden for dette modul vil vi diskutere yderligere, hvordan du filmer dit videoindhold, ved at bruge den bedste positionering, belysning og vinkler samt de mobile apps, som kan gøre dit liv lettere, når du laver videomarkedsføringsindhold i høj kvalitet!

3.2 Integrering og re-udarbejdelse af digitalt indhold

Enhed 3.2	Integrering og re-udarbejdelse af digitalt indhold

[14] https://www.globalmediainsight.com/blog/youtube-users-statistics/

Varighed	2,5 timer
Mål	Præsentation af typiske former for indholdsskabelse og dets lagring. Angivelse af, hvordan man kan publicere og vedligeholde indhold på internettet.
Indhold	Power point-ressourcer (download fra hjemmesiden) Autonome, fleksible ressourcer, der kan bruges på farten - E-Learning
Ressourcer	PC/mobil eller tablet til e-learning
Træningsmetoder	Præsentation af træner Præsentation af deltagere

Bord18Kompetenceenhedens struktur 3.2. – Integrering og re-udarbejdelse af digitalt indhold i Modul 3 – Indholdsskabelse.

3.2 Integrering og re-udarbejdelse af digitalt indhold

Indholdsskabelse og integration. At ændre, forfine og integrere ny information og indhold i en eksisterende mængde viden og ressourcer for at skabe nyt, originalt og relevant indhold og viden.

Vi har berørt skabelsen af meget engagerende indhold til dit publikum, under hensyntagen til konteksten for din brug. Hvem prøver du at nå? Brug dine styrker til at nå ud til din målgruppe, foretag nogle markedsundersøgelser for at sikre, at du træffer det rigtige valg for dig! Vi vil også dække publicering og opbevaring af indhold online. Inden for at integrere dit indhold i allerede eksisterende ressourcer vil vi vise dig, hvordan du bruger produktivitetssoftware og apps til at opnå dette på en effektiv og brugbar måde! Brug af værktøjer, som allerede eksisterer, betyder, at du vil bruge mindre kapital og energi, mens du stadig opnår det endelige mål, som er at skabe indhold, der er yderst engagerende, der opfylder dine behov og behovene hos din målgruppe!

Som vi har været inde på før, YouTube har en massiv bank af materialer, offentligt tilgængeligt, som kan være yderst nyttigt, Podcast-indhold er også frit tilgængeligt og kan hjælpe med at supplere de ressourcer, du opretter.

Igennem 3.2 vil du blive introduceret til et væld af nyttige værktøjer, som vil gøre din rejse med indholdsintegration og udarbejdelse meget mere spændende og problemfri.

- En note
- Evernote
- Draw.io
- PIXLR
- Adobe Spark
- Google Docs

Lagring af dit indhold

Når du har brugt din tid og energi på at skabe og integrere dit digitale indhold, er det yderst vigtigt, at du har færdighederne og viden om, hvor det er sikrest at gemme dette indhold for nem adgang, men også sikkerhed.

Cloud fildeling kan være en nyttig platform, som giver brugerne mulighed for at få adgang til deres indhold fra enhver enhed, denne fleksibilitet betyder, at du ikke er bundet til en fysisk pc og er af yderste vigtighed i et dynamisk og hvert skiftende arbejdsområde. Oplev Dropbox, Google Drive og One Drive, og skift måden, du deler dine materialer på.

Udgivelse og deling

At dele dine kreationer online er processen med at publicere indhold på online platforme, det være sig en YouTube-kanal, din egen personlige hjemmeside og blogside eller din sociale mediekonto. Udgivet indhold kan omfatte tekst, billeder, videoer og andre typer digitale medier.

At publicere online kan være billigt, yderst effektivt og effektivt til din brug, så vi kan hjælpe dig med at finde de bedste værktøjer til at publicere. Lær mere om WIX, Wordpress, Linkedin og Pinterest.

3.3 Copyright og licenser

Enhed 3.3	Copyright og licenser
Varighed	2,5 timer
Mål	Ophavsret er en form for intellektuel ejendomsret (IPR), der giver beskyttelse over noget: • du kan skabe • ejet af en eller flere personer eller virksomheder
Indhold	Autonome, fleksible ressourcer, der kan bruges på farten - E-Learning
Ressourcer	Power point-ressourcer (download fra hjemmesiden) PC/mobil eller tablet til e-learning
Træningsmetoder	Præsentation af træner

Bord19 - Kompetenceenhedens struktur 3.3.- Ophavsret og licenser til Modul 3 – Indholdsoprettelse.

3.3 Copyright og licenser

Hvad er ophavsret?

Ophavsret giver ejeren eneret til at bruge værket, med nogle undtagelser. Når en person skaber et originalt værk, fastgjort i et håndgribeligt medie, ejer han eller hun automatisk ophavsretten til værket.

Mange typer værker er berettiget til ophavsretlig beskyttelse, for eksempel:

- Audiovisuelle værker, såsom tv-programmer, film og onlinevideoer
- Lydoptagelser og musikalske kompositioner
- Skriftlige værker, såsom foredrag, artikler, bøger og musikalske kompositioner
- Visuelle værker, såsom malerier, plakater og reklamer
- Videospil og computersoftware
- Dramatiske værker, såsom skuespil og musicals

Er det muligt at bruge et ophavsretligt beskyttet værk uden at krænke det?

Ja, under nogle omstændigheder er det muligt at bruge et ophavsretligt beskyttet værk uden at krænke ejerens ophavsret. Nogle indholdsskabere vælger at gøre deres arbejde tilgængeligt til genbrug med visse krav. For mere om dette, kan du ønske at lære omCreative Commons-licens.[15]

Den Europæiske Unions lov om ophavsret

Den Europæiske Unions ophavsretslov erophavsretgældende lovgivning inden foreuropæiske Union. Ophavsretslovgivningen er stort set harmoniseret i Unionen, selvom der er forskelle fra land til land. Lovsamlingen blev implementeret i EU gennem en rækkedirektiver, som medlemslandene skal indføre i deres nationale lovgivning. De vigtigste copyright-direktiver erDirektiv om ophavsretsbegreber, detInformationssamfundsdirektivetogDirektiv om ophavsret i det digitale indre marked.[16]

EU's lov om ophavsret består af 11 direktiver og 2 forordninger, der harmoniserer de væsentlige rettigheder for ophavsmænd, udøvende kunstnere, producenter og tv-selskaber. Ved at fastsætte harmoniserede standarder reducerer EU's ophavsretslovgivning nationale uoverensstemmelser og garanterer det nødvendige beskyttelsesniveau for at fremme kreativitet og investering i kreativitet. Harmoniserede standarder fremmer

[15] https://support.google.com/legal/answer/3463239?hl=da-DK

[16] https://en.wikipedia.org/wiki/Copyright_law_of_the_European_Union

kulturel mangfoldighed og giver forbrugere og virksomheder bedre adgang til digitalt indhold og tjenester i hele Europa.[17]

Inden for 3.3 vil vi dykke dybere ned i kravene til ophavsret, hvordan man bruger en creative commons-licens, og hvordan disse typer licenser kan være nyttige for dit indhold!

3.4 Programmering

Enhed 3.4	Programmering
Varighed	2,5 timer
Mål	Formålet med dette modul er at få en forståelse af grundlæggende strukturer i Python-sproget.
Indhold	Autonome, fleksible ressourcer, der kan bruges på farten - E-Learning
Ressourcer	Power point-ressourcer (download fra hjemmesiden) PC/mobil eller tablet til e-learning
Træningsmetoder	Præsentation af træner Flæbede klasseværelse

Bord20- Kompetenceenhedens opbygning 3.4. - Programmering af modul 3 – Indholdsskabelse.

3.4 Grundlæggende programmering og kodning

Hvad er programmering på et grundlæggende niveau?

Kodning er en grundlæggende læsefærdighed i den digitale tidsalder, og det er vigtigt for hver person at forstå og være i stand til simpel kodning og bruge teknologi omkring sig. Der er mange forskellige kodningssprog. Vi valgte Python. Python er en enkel og nem at lære på grund af dens klare syntaks og læsbarhed.

[17] https://digital-strategy.ec.europa.eu/da/policies/copyright-legislation

Python er et let at lære, kraftfuldt programmeringssprog.

Python er et programmeringssprog, der er nemt at lære og kraftfuldt i drift. Mens du skriver koden, vil du primært være fokuseret på at løse problemet, ikke på syntaksen og strukturen af det sprog, du programmerer på.

Python-variabler

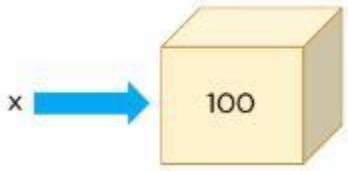
1. Variabel tildeling

En variabel er et grundlæggende koncept i ethvert programmeringssprog. Det er en reserveret hukommelsesplacering, der gemmer og manipulerer data. Tænk på en variabel som et navn knyttet til et bestemt objekt. I Python behøver variabler ikke deklareres eller defineres på forhånd, som det er tilfældet i mange andre programmeringssprog. For at oprette en variabel skal du blot tildele den en værdi og derefter begynde at bruge den. Tildeling udføres med et enkelt lighedstegn (=):

Variabler er enheder af et program, der har en værdi. Her er et eksempel på en variabel:

x=100

I nedenstående diagram har boksen en værdi på 100 og er navngivet som x. Derfor er variablen x, og de data, den indeholder, er værdien.



Datatypen for en variabel er den type data, den har.18

I ovenstående eksempel holder x 100, som er et tal, og datatypen x er et tal.

I Python er der tre typer tal: heltal, flydende og kompleks.

[18] https://www.simplilearn.com/tutorials/python-tutorial/python-variables

Heltal er tal uden decimaltegn. Floats er tal med decimaler. Komplekse tal har reelle dele og imaginære dele.

En anden datatype, der er meget forskellig fra et tal, kaldes en streng, som er en samling af tegn.

Lad os se en variabel med en heltalsdatatype:

x=100

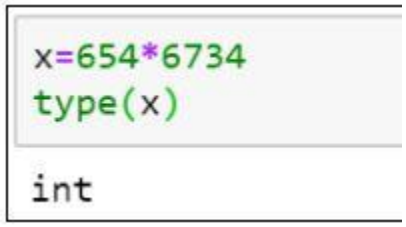
For at kontrollere datatypen for x skal du bruge type()-funktionen:

type(x)

Python giver dig mulighed for at tildele variabler, mens du udfører aritmetiske operationer.

x=654*6734

type(x)



For at vise outputtet af variablen, brug print()-funktionen.

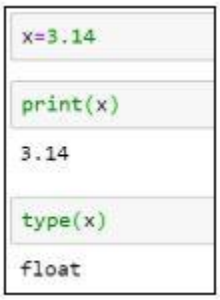
print(x) #Det giver produktet af de to tal

Lad os nu se et eksempel på et flydende kommatal:

x=3,14

print(x)

type(x) #Her typen variablen er float



Strenge erklæres inden for et enkelt eller dobbelt anførselstegn.

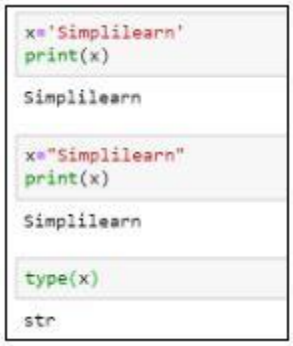
x='Simplilearn'

print(x)

x=" Simplilearn."

print(x)

type(x)



For at lære mere har vi linket en interessant side med fremragende infografik:

https://realpython.com/python-variables/

Tillykke, du har nu gennemført modul 3.

Glem ikke at tjekke bilagene for yderligere ressourcer og dokumenter til støtte for selvstudium!

Modul 4: Sikkerhed

Modul 4 er fokuseret på sikkerhed online og har til formål at henlede din opmærksomhed på dette problem sammen med at give dig information om, hvordan du reducerer risici og bevarer din sikkerhed.

Bemærk venligst, at praktiske aktiviteter beskrevet i hver enhed kan indebære støtte fra en erfaren træner. Selvom oplysningerne i manualen er skrevet på en måde, der er let at forstå, kan nogle handlinger, der støder op til de præsenterede oplysninger, kræve støtte fra erfarne personer.

Modul 4	**Sikkerhed**			
Varighed	**25 timer**			
Mål	Inden for denne enhed vil deltageren blive trænet i at: • at beskytte enheder, indhold, personlige data og privatliv i digitale miljøer; • at beskytte fysisk og psykisk sundhed og være opmærksom på digitale teknologier til socialt velvære og social inklusion; • at være opmærksom på miljøpåvirkningen af digitale teknologier og deres anvendelse.			
Enheder	4.1 Beskyttelse af enheder	4.2 Beskyttelse af personlige data og privatliv	4.3 Beskyttelse af sundhed og velvære	4.4 Beskyttelse af miljøet
Træningsorganisation	Ansigt til ansigt E-læring B-læring	Ansigt til ansigt E-læring B-læring	Ansigt til ansigt E-læring B-læring	Ansigt til ansigt E-læring B-læring
Varighed	6 timer	9 timer	5 timer	5 timer

Bord 21 - Global struktur af Modul 4 – Sikkerhed.

4.1 Beskyttelse af enheder

Enhed 4.1	Beskyttelse af enheder
Varighed	6 timer
Mål	At forstå, at en computer er tilbøjelig til netværkscyberangreb At vide, hvordan man opretter en stærk adgangskode For at kunne installere en Chrome-internetbrowser og opdatere den med jævne mellemrum At forstå den indsats, det menneskelige øje gør for at læse information fra elektroniske enheder Forstå, at en forkert arbejdsstilling kan føre til medicinske problemer med rygsøjlen For at forstå udstyrets driftsomkostninger At forstå, at fysiske elektroniske komponenter ikke er "miljøvenlige"
Indhold	4.1.1 Beskyttelse af enheder 4.1.2 Softwareopdateringer 4.1.3. Sikkerhed og adgangskoder 4.1.4 Øget sikkerhed 4.1.5 Hvad er en ondsindet kode? 4.1.6 Praktiske aktiviteter
Ressourcer	Træningsmanual Computer med internetadgang Redigeringsprogram Papirer kuglepenne
Træningsmetoder	Præsentation af træner Medievalg

Bord 22- Kompetenceenhedens opbygning 4.1. – Beskyttelsesanordninger i modul 4 – Sikkerhed.

4.1.1 Beskyttelse af enheder

Hvorfor er computersikkerhed vigtig?

Fordi computere spiller så kritiske roller i vores liv, og fordi vi indtaster og ser så mange personligt identificerbare oplysninger om dem, er det bydende nødvendigt at implementere og vedligeholde computersikkerhed. Stærk computersikkerhed sikrer sikker behandling og opbevaring af vores oplysninger.

Hvordan kan jeg forbedre min computers sikkerhed?

Følgende er vigtige trin, du bør overveje for at gøre din computer mere sikker. Selvom intet individuelt trin vil eliminere alle risici, når de bruges sammen, vil disse dybtgående forsvarsmetoder styrke din computers sikkerhed og hjælpe med at minimere trusler.

➢ Sikre dit hjemmenetværk

Når du forbinder en computer til internettet, er den også forbundet til millioner af andre computere – en forbindelse, der kan give angribere adgang til din computer. Selvom kabelmodemmer, digitale abonnentlinjer (DSL'er) og internetudbydere (ISP'er) har et vist niveau af sikkerhedsovervågning, er det afgørende at sikre din router - den første sikrede enhed, der modtager information fra internettet. Sørg for at sikre den, før du opretter forbindelse til internettet for at styrke din computers sikkerhed.
Hvad er hjemmenetværkssikkerhed, og hvorfor skal jeg bekymre mig?

➢ Hjemmenetværkssikkerhed

Hjemmenetværkssikkerhed refererer til beskyttelsen af et netværk, der forbinder enheder – såsom routere, computere, smartphones, husholdningsapparater, Wi-Fi-aktiverede babyalarmer, kameraer – til hinanden og til internettet i et hjem.
Mange hjemmebrugere deler to almindelige misforståelser om sikkerheden på deres netværk:

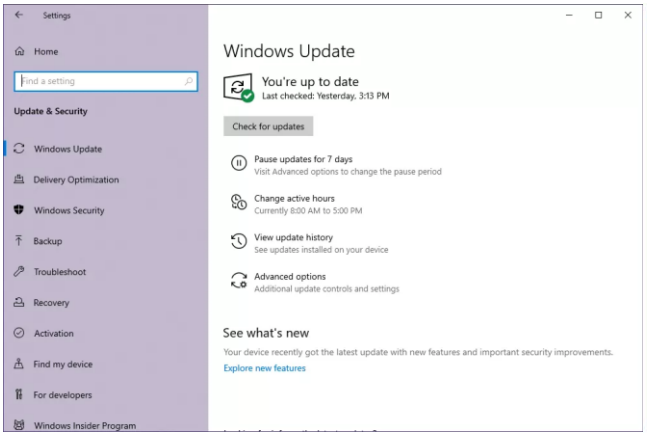
- Deres hjemmenetværk er for lille til at være i fare for et cyberangreb.
- Deres enheder er "sikre nok" lige ud af kassen.

De fleste angreb er ikke af personlig karakter og kan forekomme på enhver type netværk – store som små, hjemme eller i virksomheden. Hvis et netværk opretter forbindelse til internettet, er det i sagens natur mere sårbart og modtageligt over for trusler udefra.
Hvordan forbedrer jeg sikkerheden på mit hjemmenetværk?
Ved at følge nogle af de enkle, men effektive afbødningsteknikker nedenfor, kan du reducere angrebsoverfladen på dit hjemmenetværk betydeligt og gøre det sværere for en ondsindet cyberaktør at iværksætte et vellykket angreb.

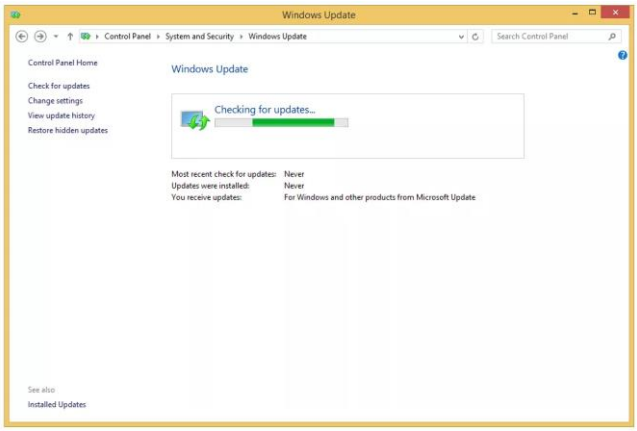
➢ Opdater din software regelmæssigt

Regelmæssige softwareopdateringer er et af de mest effektive trin, du kan tage for at forbedre den overordnede cybersikkerhedsposition for dine hjemmenetværk og -systemer. Udover at tilføje nye funktioner og funktionalitet inkluderer softwareopdateringer ofte kritiske patches og sikkerhedsrettelser til nyopdagede trusler og sårbarheder. De fleste moderne softwareapplikationer vil automatisk søge efter nyligt udgivne opdateringer.

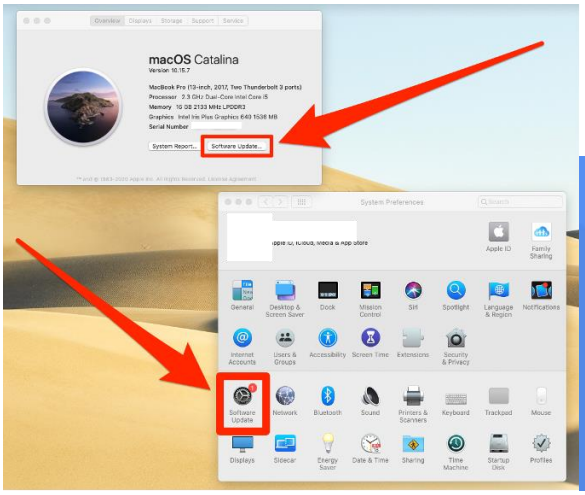
Hvis automatiserede opdateringer ikke er tilgængelige, kan du overveje at købe et softwareprogram, der identificerer og centralt administrerer alle installerede softwareopdateringer.



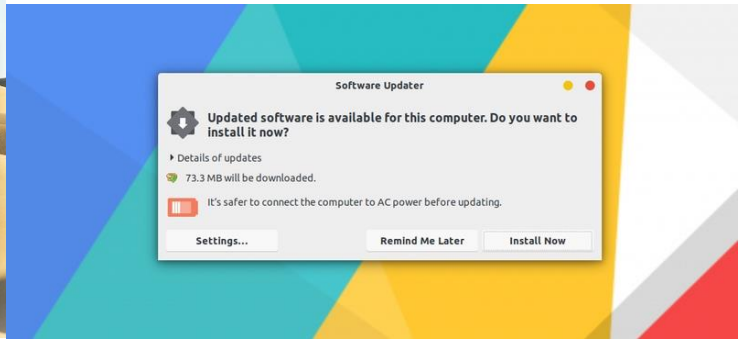
Windows 10



Windows 8,7, Vista



MacOS-opdatering



Ubuntu (Linux) opdatering

Hvad er patches?

Patches er software- og operativsystemopdateringer, der adresserer sikkerhedssårbarheder i et program eller et produkt. Softwareleverandører kan vælge at frigive opdateringer for at rette ydeevnefejl samt for at levere forbedrede sikkerhedsfunktioner.

4.1.2 Softwareopdateringer

Hvordan finder du ud af, hvilke softwareopdateringer du skal installere?

Når softwareopdateringer bliver tilgængelige, sætter leverandører dem normalt på deres websteder, så brugerne kan downloade dem. Installer opdateringer så hurtigt som muligt for at beskytte din computer, telefon eller anden digital enhed mod angribere, der ville drage fordel af systemets sårbarheder. Angribere kan målrette mod sårbarheder i måneder eller endda år efter, at opdateringer er tilgængelige.

Noget software vil automatisk søge efter opdateringer, og mange leverandører tilbyder brugerne muligheden for at modtage opdateringer automatisk. Hvis automatiske muligheder er tilgængelige, kan du drage fordel af dem. Hvis de ikke er tilgængelige, skal du jævnligt tjekke din leverandørs websteder for opdateringer.

Sørg for, at du kun downloader softwareopdateringer fra betroede leverandørers websteder. Stol ikke på et link i en e-mail-angribere har brugt e-mail-meddelelser til at dirigere brugere til websteder, der hoster ondsindede filer forklædt som legitime opdateringer. Brugere bør også være mistænksomme over for e-mails, der hævder at have en softwareopdateringsfil vedhæftet – disse vedhæftede filer kan indeholde malware.

Hvis det er muligt, skal du kun anvende automatiske opdateringer fra betroede netværksplaceringer (f.eks. hjemme, arbejde). Undgå at opdatere software (automatisk eller manuelt), mens du er tilsluttet upålidelige netværk (f.eks. lufthavn, hotel, kaffebar). Hvis opdateringer skal installeres over et netværk, der ikke er tillid til, skal du bruge en Virtual Private Network-forbindelse til et pålideligt netværk og anvende opdateringer.

Hvad er forskellen mellem manuelle og automatiske opdateringer?

Brugere kan installere opdateringer manuelt eller vælge, at deres softwareprogrammer skal opdateres automatisk.

Manuelle opdateringer kræver, at brugeren eller administratoren besøger leverandørens websted for at downloade og installere softwarefiler.

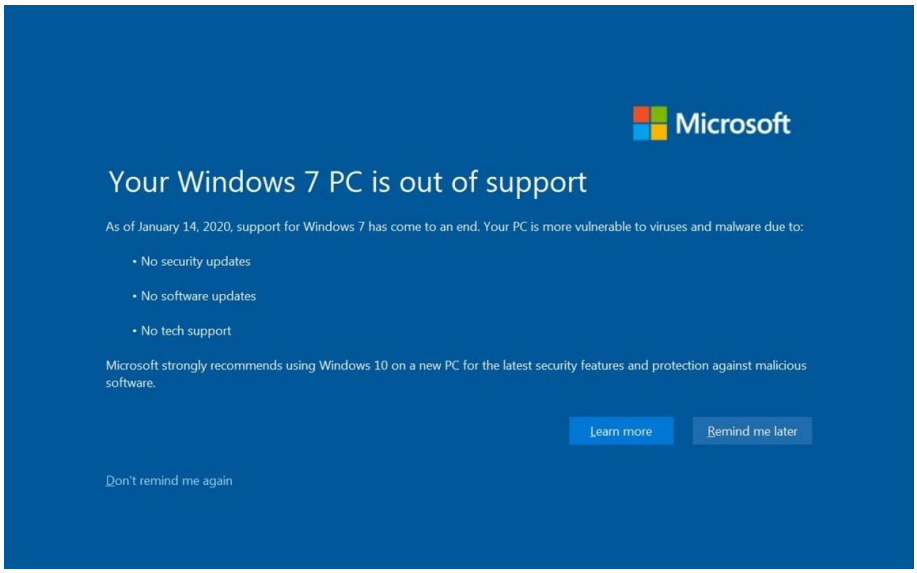
Automatiske opdateringer kræver bruger- eller administratorsamtykke, når softwaren installeres eller konfigureres. Når du giver samtykke til automatiske opdateringer, "skubbes" (eller installeres) softwareopdateringer til dit system automatisk.

Hvad er end-of-life software?

Nogle gange vil leverandører afbryde support til et softwareprogram eller udstede softwareopdateringer til det (også kendt som end-of-life [EOL]-software). Fortsat brug af EOL-software udgør en følgerisiko for dit system, som kan tillade en hacker at udnytte sikkerhedssårbarheder. Brugen af ikke-understøttet software kan også forårsage problemer med softwarekompatibilitet samt nedsat systemydeevne og produktivitet.

Bedste praksis for softwareopdateringer

- Aktiver automatiske softwareopdateringer, når det er muligt. Dette vil sikre, at softwareopdateringer installeres så hurtigt som muligt.
- Brug ikke ikke-understøttet EOL-software.
- Besøg altid leverandørwebsteder direkte i stedet for at klikke på annoncer eller e-mail-links.
- Undgå softwareopdateringer, mens du bruger ikke-pålidelige netværk.
- Nye sårbarheder dukker hele tiden op, men det bedste forsvar mod angribere, der udnytter lappede sårbarheder, er enkelt: Hold din software opdateret. Dette er den mest effektive foranstaltning, du kan tage for at beskytte din computer, telefon og andre digitale enheder.



Windows 7 EOL

Fjern unødvendige tjenester og software

Deaktiver alle unødvendige tjenester for at reducere angrebsoverfladen på dit netværk og enheder, inklusive din router. Ubrugte eller uønskede tjenester og software kan skabe sikkerhedshuller på en enheds system, hvilket kan føre til en øget angrebsoverflade af dit netværksmiljø. Dette er især tilfældet med nye computersystemer, hvor leverandører ofte vil forudinstallere et stort antal prøvesoftware og -applikationer - kaldet "bloatware" - som brugerne måske ikke finder nyttige.

Juster fabriksstandardkonfigurationer på software og hardware

Mange software- og hardwareprodukter kommer "ud af boksen" med alt for tilladelige fabriksstandardkonfigurationer beregnet til at gøre dem brugervenlige og reducere fejlfindingstiden for kundeservice. Desværre er disse standardkonfigurationer ikke rettet mod sikkerhed. At lade dem være aktiveret efter installationen kan skabe flere muligheder for en angriber at udnytte. Brugere bør tage skridt til at skærpe standardkonfigurationsparametrene for at reducere sårbarheder og beskytte mod indtrængen.

4.1.3 Sikkerhed og adgangskoder

Skift standard login-adgangskoder og brugernavne

De fleste netværksenheder er forudkonfigureret med standardadministratoradgangskoder for at forenkle opsætningen. Disse standardlegitimationsoplysninger er ikke sikre - de kan være let tilgængelige på internettet, eller de kan endda være fysisk mærket på selve enheden. At lade disse være uændrede skaber muligheder for ondsindede cyberaktører til at få uautoriseret adgang til information, installere skadelig software og forårsage andre problemer.

Brug stærke og unikke adgangskoder

Vælg stærke adgangskoder for at hjælpe med at sikre dine enheder. Derudover må du ikke bruge den samme adgangskode med flere konti. På denne måde, hvis en af dine konti er kompromitteret, vil angriberen ikke være i stand til at krænke andre af dine konti.

Hvorfor har du brug for stærke adgangskoder?

Du bruger sandsynligvis personlige identifikationsnumre (PIN'er), adgangskoder eller adgangssætninger hver dag: fra at få penge fra pengeautomaten eller bruge dit betalingskort i en butik, til at logge ind på din e-mail eller i en online forhandler. Det kan være frustrerende at spore alle tal-, bogstav- og ordkombinationer, men disse beskyttelser er vigtige, fordi hackere udgør en reel trussel mod dine oplysninger. Ofte handler et angreb ikke specifikt om din konto, men om at bruge adgangen til dine oplysninger til at iværksætte et større angreb.

En af de bedste måder at beskytte information eller fysisk ejendom på er at sikre, at kun autoriserede personer har adgang til dem. Det næste skridt er at bekræfte, at de, der anmoder om adgang, er de personer, de hævder at være. Denne autentificeringsproces er vigtigere og sværere i cyberverdenen. Adgangskoder er det mest almindelige middel til godkendelse, men fungerer kun, hvis de er komplekse og fortrolige. Mange systemer og tjenester er blevet brudt med succes på grund af usikre og utilstrækkelige adgangskoder. Når først et system er kompromitteret, er det åbent for udnyttelse af andre uønskede kilder.

Undgå almindelige fejl

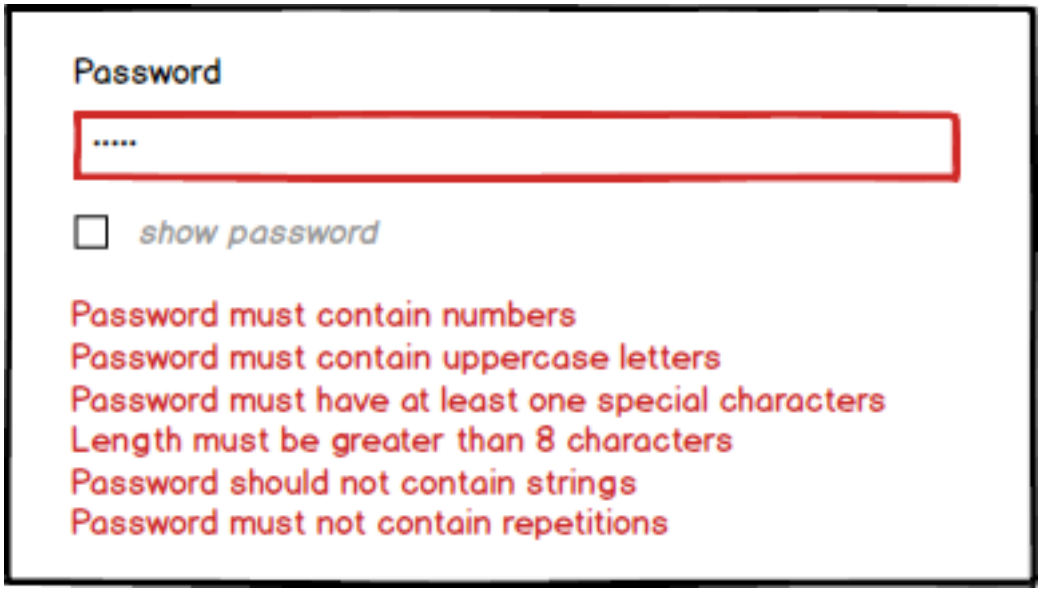
De fleste bruger adgangskoder, der er baseret på personlige oplysninger og er nemme at huske. Det gør det dog også nemmere for en angriber at knække dem. Overvej en firecifret pinkode. Er din en kombination af måneden, dagen eller året for din fødselsdag? Indeholder den din adresse eller dit telefonnummer? Tænk på, hvor nemt det er at finde en persons fødselsdag eller lignende information. Hvad med din e-mail-adgangskode - er det et ord, der kan findes i ordbogen? Hvis det er tilfældet, kan det være modtageligt for ordbogsangreb, som forsøger at gætte adgangskoder baseret på almindelige ord eller sætninger.

Selvom bevidst stavefejl af et ord ("daytt" i stedet for "dato") kan give en vis beskyttelse mod ordbogsangreb, er en endnu bedre metode at stole på en række ord og bruge hukommelsesteknikker eller mnemonics til at hjælpe dig med at huske, hvordan du afkoder det. Brug f.eks. "IlTpbb" i stedet for adgangskoden "hoops" for "[I] [l]like

[T]o [p]lay [b]asket[b]all." Brug af både små og store bogstaver tilføjer endnu et lag af uklarhed. Ændring af det samme eksempel brugt ovenfor til "Il!2pBb." opretter en adgangskode, der er meget forskellig fra ethvert ordbogsord.

Længde og kompleksitet

Du bør overveje at bruge den længste tilladte adgangskode eller adgangssætning (8–64 tegn), når du kan. For eksempel "Pattern2baseball#4mYmiemale!" ville være en stærk adgangskode, fordi den har 28 tegn og indeholder store og små bogstaver, tal og specialtegn. Du skal muligvis prøve forskellige varianter af en adgangssætning – for eksempel begrænser nogle programmer længden af adgangskoder, og nogle accepterer ikke mellemrum eller visse specialtegn. Undgå almindelige sætninger, berømte citater og sangtekster.



Må og lad være

Når du først har fundet frem til en stærk, mindeværdig adgangskode, er det fristende at genbruge den – lad være! Genbrug af en adgangskode, selv en stærk, bringer dine konti lige så meget i fare som at bruge en svag

adgangskode. Hvis angribere gætter din adgangskode, ville de have adgang til dine andre konti med den samme adgangskode. Brug følgende teknikker til at udvikle unikke adgangskoder til hver af dine konti:

- Brug forskellige adgangskoder på forskellige systemer og konti.
- Brug den længste adgangskode eller adgangssætning, der er tilladt for hvert adgangskodesystem.
- Udvikl mnemonics til at huske komplekse adgangskoder.
- Overvej at bruge et adgangskodehåndteringsprogram til at holde styr på dine adgangskoder. (Se mere information nedenfor.)
- Brug ikke adgangskoder, der er baseret på personlige oplysninger, der let kan tilgås eller gættes.
- Brug ikke ord, der kan findes i nogen ordbog på ethvert sprog.

Sådan beskytter du dine adgangskoder

Efter at have valgt en adgangskode, der er let at huske, men svær for andre at gætte, skal du ikke skrive den ned og efterlade den et sted, hvor andre kan finde den. Hvis du skriver det ned og efterlader det på dit skrivebord, ved siden af din computer, eller endnu værre, tapet til din computer, gør det let tilgængeligt for en person med fysisk adgang til dit kontor. Fortæl ikke nogen dine adgangskoder, og hold øje med angribere, der forsøger at narre dig gennem telefonopkald eller e-mails, der anmoder om, at du afslører dine adgangskoder.

Programmer kaldet password managers tilbyder muligheden for at oprette tilfældigt genererede passwords til alle dine konti. Du får derefter adgang til de stærke adgangskoder med en hovedadgangskode. Hvis du bruger en adgangskodehåndtering, skal du huske at bruge en stærk hovedadgangskode.

Adgangskodeproblemer kan stamme fra din webbrowsers evne til at gemme adgangskoder og dine onlinesessioner i hukommelsen. Afhængigt af din webbrowsers indstillinger kan alle med adgang til din computer muligvis opdage alle dine adgangskoder og få adgang til dine oplysninger. Husk altid at logge ud, når du bruger en offentlig computer (på biblioteket, en internetcafé eller endda en delt computer på dit kontor). Undgå at bruge offentlige computere og offentlig Wi-Fi til at få adgang til følsomme konti såsom bank og e-mail.

Der er ingen garanti for, at disse teknikker forhindrer en hacker i at lære dit kodeord, men de vil gøre det sværere.

Glem ikke grundlæggende sikkerhed

- Hold dit operativsystem, browser og anden software opdateret.
- Brug og vedligehold antivirussoftware og en firewall.
- Scan regelmæssigt din computer for spyware. (Nogle antivirusprogrammer indeholder spywaredetektion.)
- Vær forsigtig med vedhæftede filer i e-mails og upålidelige links.

4.1.4 Øget sikkerhed

Kør opdateret antivirussoftware

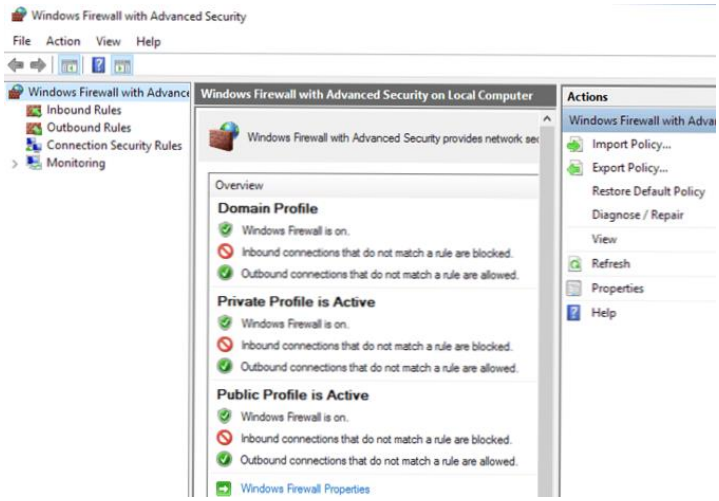
En velrenommeret antivirussoftwareapplikation er en vigtig beskyttelsesforanstaltning mod kendte ondsindede trusler. Det kan automatisk opdage, sætte i karantæne og fjerne forskellige typer malware, såsom vira, orme og løsepenge. Mange antivirusløsninger er ekstremt nemme at installere og intuitive at bruge. Det anbefales, at alle computere og mobile enheder på dit hjemmenetværk kører antivirussoftware. Sørg desuden for at aktivere automatiske virusdefinitionsopdateringer for at sikre maksimal beskyttelse mod de seneste trusler. Bemærk: Fordi detektion er afhængig af signaturer - kendte mønstre, der kan identificere kode som malware - vil selv det bedste antivirus ikke give tilstrækkelig beskyttelse mod nye og avancerede trusler, såsom nul-dages udnyttelse og polymorfe vira.

https://review-shark.com/2021-best-antivirus-software-for-computer-and-laptop/

Installer en netværksfirewall

Installer en firewall ved grænsen af dit hjemmenetværk for at forsvare dig mod eksterne trusler. En firewall kan blokere ondsindet trafik fra at komme ind på dit hjemmenetværk og advare dig om potentielt farlig aktivitet. Når den er korrekt konfigureret, kan den også tjene som en barriere for interne trusler, der forhindrer uønsket eller ondsindet software i at nå ud til internettet. De fleste trådløse routere kommer med en konfigurerbar, indbygget netværksfirewall, der inkluderer yderligere funktioner – såsom adgangskontrol, web-filtrering og denial-of-service (DoS)-forsvar – som du kan skræddersy til at passe til dit netværksmiljø. Husk, at nogle firewall-funktioner, inklusive selve firewallen, kan være slået fra som standard. At sikre, at din firewall er tændt, og at alle indstillinger er korrekt konfigureret, vil styrke netværkssikkerheden på dit netværk. Bemærk:

Ud over en netværksfirewall kan du overveje at installere en firewall på alle computere, der er tilsluttet dit netværk. Disse firewalls, ofte omtalt som værts- eller softwarebaserede, inspicerer og filtrerer en computers indgående og udgående netværkstrafik baseret på en forudbestemt politik eller et sæt regler. De fleste moderne Windows- og Linux-operativsystemer kommer med en indbygget, tilpasselig og funktionsrig firewall. Derudover kombinerer de fleste leverandører deres antivirussoftware med yderligere sikkerhedsfunktioner, såsom forældrekontrol, e-mail-beskyttelse og ondsindet blokering af websteder.



Sikkerhedskopier dine data regelmæssigt

Lav og gem – ved hjælp af enten eksterne medier eller en cloud-baseret tjeneste – regelmæssige sikkerhedskopier af al værdifuld information på din enhed. Overvej at bruge en tredjeparts backup-applikation, som kan forenkle og automatisere processen. Sørg for at kryptere din backup for at beskytte fortroligheden og integriteten af dine oplysninger. Datasikkerhedskopier er afgørende for at minimere virkningen, hvis disse data går tabt, beskadiges, inficeres eller stjæles.

Forøg trådløs sikkerhed

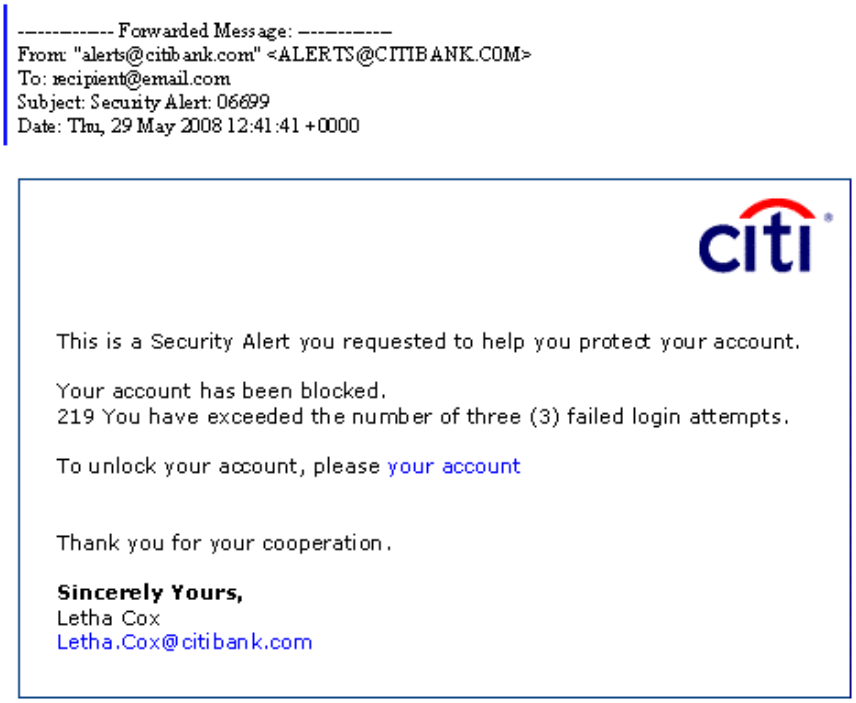
Du skal muligvis konsultere din routers brugsanvisning eller kontakte din internetudbyder for at få specifikke instruktioner om, hvordan du ændrer en bestemt indstilling på din enhed.

Brug den stærkeste tilgængelige krypteringsprotokol. Det anbefales at bruge Wi-Fi Protected Access 3 (WPA3) Personal Advanced Encryption Standard (AES) og Temporary Key Integrity Protocol (TKIP), som i øjeblikket er den mest sikre routerkonfiguration til rådighed til hjemmebrug. Den inkorporerer AES og er i stand til at bruge kryptografiske nøgler på 128, 192 og 256 bit. Denne standard er blevet godkendt af National Institute of Standards and Technology (NIST).
Skift routerens standard administratoradgangskode. Skift din routers administratoradgangskode for at hjælpe med at beskytte den mod et angreb ved hjælp af standardlegitimationsoplysninger.
Skift standardservicesæt-id'en (SSID). Nogle gange omtales som "netværksnavnet", et SSID er et unikt navn, der identificerer et bestemt trådløst lokalnetværk (WLAN). Alle trådløse enheder på et trådløst lokalnetværk (WLAN) skal bruge det samme SSID for at kommunikere med hinanden. Fordi enhedens standard-SSID typisk identificerer producenten eller den faktiske enhed, kan en angriber bruge dette til at identificere enheden og udnytte enhver af dens kendte sårbarheder. Gør dit SSID unikt og ikke bundet til din identitet eller placering, hvilket ville gøre det nemmere for angriberen at identificere dit hjemmenetværk.
Deaktiver Wi-Fi Protected Setup (WPS). WPS giver forenklede mekanismer til, at en trådløs enhed kan tilslutte sig et Wi-Fi-netværk uden at skulle indtaste adgangskoden til det trådløse netværk. En designfejl i WPS-specifikationen for PIN-godkendelse reducerer imidlertid den tid, det kræves for en cyberangriber at brute force en hel PIN-kode, fordi den informerer dem, når den første halvdel af den ottecifrede PIN-kode er korrekt. Mange routere mangler en ordentlig lockout-politik efter et vist antal mislykkede forsøg på at gætte PIN-koden, hvilket gør et brute-force-angreb meget mere sandsynligt. Se Brute Force-angreb udført af cyberaktører.
Reducer den trådløse signalstyrke. Dit Wi-Fi-signal forplanter sig ofte ud over dit hjems omkreds. Denne udvidede emission tillader aflytning af ubudne gæster uden for dit netværks perimeter. Overvej derfor omhyggeligt antenneplacering, antennetype og transmissionseffektniveauer. Ved at eksperimentere med din routerplacering og signalstyrkeniveauer kan du mindske transmissionsdækningen af dit Wi-Fi-netværk og

dermed reducere denne risiko for kompromittering. Bemærk: Selvom dette reducerer din risiko, kan en motiveret angriber muligvis stadig opsnappe et signal, der har begrænset dækning.
Sluk for netværket, når det ikke er i brug. Selvom det kan være upraktisk at slukke og tænde for Wi-Fi-signalet ofte, kan du overveje at deaktivere det under rejser eller længere perioder, hvor du ikke behøver at være online. Derudover tilbyder mange routere muligheden for at konfigurere en trådløs tidsplan, der automatisk deaktiverer Wi-Fi på bestemte tidspunkter. Når dit Wi-Fi er deaktiveret, forhindrer du eksterne angribere i at kunne udnytte dit hjemmenetværk.
Deaktiver Universal Plug and Play (UPnP), når det ikke er nødvendigt. UPnP er en praktisk funktion, der gør det muligt for netværksenheder problemfrit at opdage og etablere kommunikation med hinanden på netværket. Men selvom UPnP-funktionen letter den indledende netværkskonfiguration, er det også en sikkerhedsrisiko. Nylige storstilede netværksangreb beviser, at malware på dit netværk kan bruge UPnP til at omgå din routers firewall, tillade angribere at tage kontrol over dine enheder på afstand og sprede malware til andre enheder. Du bør derfor deaktivere UPnP, medmindre du har et specifikt behov for det.
Opgrader firmware. Tjek din routerproducents websted for at sikre, at du kører den seneste firmwareversion. Firmwareopdateringer forbedrer produktets ydeevne, retter fejl og adresserer sikkerhedssårbarheder. Bemærk: nogle routere har mulighed for at slå automatiske opdateringer til.
Deaktiver fjernstyring. De fleste routere giver mulighed for at se og ændre deres indstillinger over internettet. Slå denne funktion fra for at beskytte mod uautoriserede personer, der får adgang til og ændrer din routers konfiguration.
Overvåg for ukendte enhedsforbindelser. Brug din routerproducents websted til at overvåge for uautoriserede enheder, der tilslutter sig eller forsøger at tilslutte sig dit netværk. Se også producentens websted for tips til, hvordan du forhindrer uautoriserede enheder i at oprette forbindelse til dit netværk.

Afbød e-mailtrusler

Phishing-e-mails er fortsat en af de mest almindelige indledende angrebsvektorer, der anvendes til malware-levering og indsamling af legitimationsoplysninger. At angribe det menneskelige element – der betragtes som den svageste komponent i ethvert netværk – fortsætter med at være ekstremt effektivt. For at inficere et system skal angriberen blot overtale en bruger til at klikke på et link eller åbne en vedhæftet fil. Den gode nyhed er, at der er mange indikatorer, som du kan bruge til hurtigt at identificere en phishing-e-mail. Det bedste forsvar mod disse angreb er at blive en uddannet og forsigtig bruger og sætte dig ind i de mest almindelige elementer i et phishing-angreb.



---------- Forwarded Message: ----------
From: "alerts@citibank.com" <ALERTS@CITIBANK.COM>
To: recipient@email.com
Subject: Security Alert: 06699
Date: Thu, 29 May 2008 12:41:41 +0000

citi

This is a Security Alert you requested to help you protect your account.

Your account has been blocked.
219 You have exceeded the number of three (3) failed login attempts.

To unlock your account, please your account

Thank you for your cooperation.

Sincerely Yours,
Letha Cox
Letha.Cox@citibank.com

Undgå social engineering og phishing-angreb

Giv ikke følsomme oplysninger til andre, medmindre du er sikker på, at de faktisk er den, de udgiver sig for at være, og at de bør have adgang til oplysningerne.

Hvad er et socialt ingeniørangreb?

I et socialt ingeniørangreb bruger en angriber menneskelig interaktion (sociale færdigheder) til at indhente eller kompromittere information om en organisation eller dens computersystemer. En angriber kan virke fordringsløs og respektabel og hævder muligvis at være en ny medarbejder, reparatør eller forsker og tilbyder endda legitimationsoplysninger for at understøtte denne identitet. Men ved at stille spørgsmål kan han eller hun muligvis samle nok information til at infiltrere en organisations netværk. Hvis en angriber ikke er i stand til at

indsamle nok information fra én kilde, kan han eller hun kontakte en anden kilde inden for samme organisation og stole på oplysningerne fra den første kilde for at øge hans eller hendes troværdighed.

Hvad er et phishing-angreb?

Phishing er en form for social engineering. Phishing-angreb bruger e-mail eller ondsindede websteder til at anmode om personlige oplysninger ved at udgive sig for at være en pålidelig organisation. For eksempel kan en angriber sende e-mail tilsyneladende fra et velrenommeret kreditkortselskab eller finansiel institution, der anmoder om kontooplysninger, hvilket ofte tyder på, at der er et problem. Når brugere svarer med de anmodede oplysninger, kan angribere bruge dem til at få adgang til konti.

Phishing-angreb kan også se ud til at komme fra andre typer organisationer, såsom velgørende organisationer. Angribere udnytter ofte aktuelle begivenheder og bestemte tidspunkter på året, som f.eks

- Naturkatastrofer (f.eks. orkanen Katrina, indonesisk tsunami)
- Epidemier og sundhedsfare (f.eks. H1N1, COVID-19)
- Økonomiske bekymringer (f.eks. IRS-svindel)
- Store politiske valg
- Helligdage

Hvad er et vishing-angreb?

Vishing er den sociale ingeniørtilgang, der udnytter stemmekommunikation. Denne teknik kan kombineres med andre former for social engineering, der lokker et offer til at ringe til et bestemt nummer og videregive følsomme oplysninger. Avancerede vishing-angreb kan foregå fuldstændigt over stemmekommunikation ved at udnytte Voice over Internet Protocol (VoIP) løsninger og udsendelsestjenester. VoIP tillader nemt opkaldsidentitet (ID) at blive forfalsket, hvilket kan drage fordel af offentlighedens fejlplacerede tillid til sikkerheden af telefontjenester, især fastnettjenester. Fastnetkommunikation kan ikke aflyttes uden fysisk adgang til linjen; denne egenskab er dog ikke gavnlig, når du kommunikerer direkte med en ondsindet skuespiller.

Hvad er et smishing attack?

Smishing er en form for social engineering, der udnytter SMS eller tekstbeskeder. Tekstbeskeder kan indeholde links til sådanne ting som websider, e-mailadresser eller telefonnumre, der, når de klikkes, automatisk åbner et browservindue eller en e-mailbesked eller ringer til et nummer. Denne integration af e-mail, tale, tekstbeskeder og webbrowserfunktionalitet øger sandsynligheden for, at brugere bliver ofre for konstrueret ondsindet aktivitet.

Hvad er almindelige indikatorer for phishingforsøg?

Mistænkelig afsenderens adresse. Afsenderens adresse kan efterligne en lovlig virksomhed. Cyberkriminelle bruger ofte en e-mailadresse, der ligner en fra et velrenommeret firma ved at ændre eller udelade nogle få tegn.

Generiske hilsner og underskrift. Både en generisk hilsen - såsom "Kære værdsatte kunde" eller "Herr/fru" - og mangel på kontaktoplysninger i signaturblokken er stærke indikatorer på en phishing-e-mail. En betroet organisation vil normalt henvende dig ved navn og give deres kontaktoplysninger.

Forfalskede hyperlinks og websteder. Hvis du holder markøren over et link i e-mailens brødtekst, og linkene ikke matcher den tekst, der vises, når du holder markøren over dem, kan linket være forfalsket. Ondsindede websteder kan se identiske ud med et legitimt websted, men URL'en kan bruge en variation i stavemåden eller et andet domæne (f.eks. .com vs. .net). Derudover kan cyberkriminelle bruge en URL-forkortelsestjeneste til at skjule den sande destination for linket.

Stavemåde og layout. Dårlig grammatik og sætningsstruktur, stavefejl og inkonsekvent formatering er andre indikatorer for et muligt phishing-forsøg. Velrenommerede institutioner har dedikeret personale, der producerer, verificerer og korrekturlæser kundekorrespondance.

Mistænkelige vedhæftede filer. En uopfordret e-mail, der anmoder en bruger om at downloade og åbne en vedhæftet fil, er en almindelig leveringsmekanisme for malware. En cyberkriminel kan bruge en falsk følelse af uopsættelighed eller vigtighed for at hjælpe med at overtale en bruger til at downloade eller åbne en vedhæftet fil uden at undersøge den først.

Hvordan undgår du at blive et offer?

Vær mistænksom over for uopfordrede telefonopkald, besøg eller e-mails fra enkeltpersoner, der spørger om medarbejdere eller andre interne oplysninger. Hvis en ukendt person hævder at være fra en legitim organisation, så prøv at bekræfte hans eller hendes identitet direkte med virksomheden.

Giv ikke personlige oplysninger eller oplysninger om din organisation, herunder dens struktur eller netværk, medmindre du er sikker på en persons autoritet til at have oplysningerne.

Afslør ikke personlige eller økonomiske oplysninger i e-mail, og svar ikke på e-mail-opfordringer om disse oplysninger. Dette inkluderer følgende links sendt i e-mail.

Send ikke følsomme oplysninger over internettet, før du har tjekket et websteds sikkerhed. (Se Beskyttelse af dit privatliv for at få flere oplysninger.)

Vær opmærksom på Uniform Resource Locator (URL) på et websted. Se efter webadresser, der begynder med "https" - en indikation af, at websteder er sikre - i stedet for "http".

Se efter et lukket hængelåsikon - et tegn på, at dine oplysninger bliver krypteret.

Hvis du er usikker på, om en e-mail-anmodning er legitim, kan du prøve at bekræfte den ved at kontakte virksomheden direkte. Brug ikke kontaktoplysninger på et websted, der er forbundet med anmodningen; tjek i stedet tidligere udsagn for kontaktoplysninger.

Installer og vedligehold antivirussoftware, firewalls og e-mailfiltre for at reducere noget af denne trafik.

Udnyt alle anti-phishing-funktioner, der tilbydes af din e-mail-klient og webbrowser.

Håndhæv multifaktorgodkendelse (MFA).

Hvad gør du, hvis du tror, du er et offer?

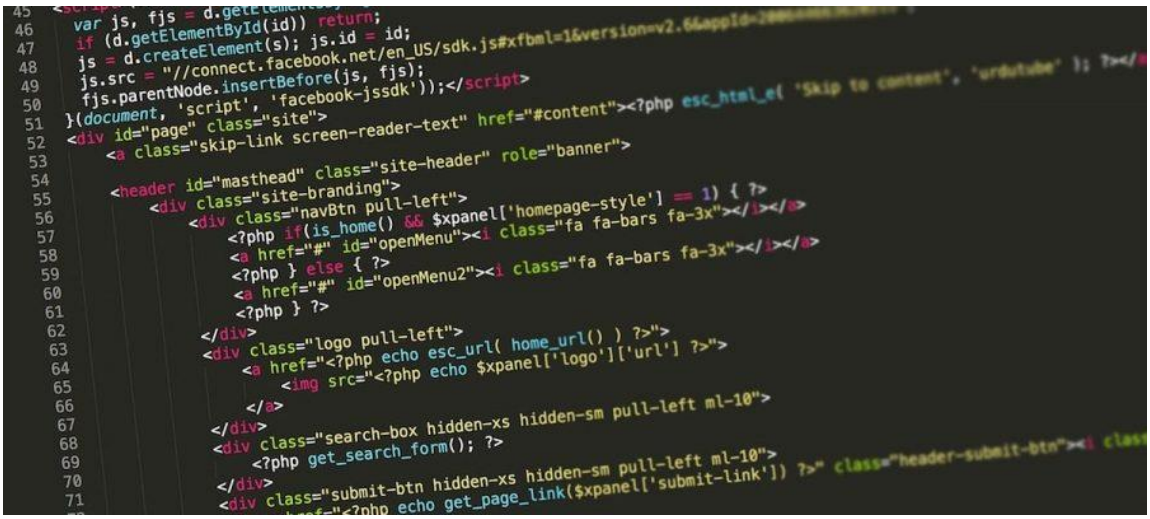
Hvis du mener, at du muligvis har afsløret følsomme oplysninger om din organisation, skal du rapportere det til de relevante personer i organisationen, herunder netværksadministratorer. De kan være opmærksomme på enhver mistænkelig eller usædvanlig aktivitet.

Hvis du mener, at dine finansielle konti kan være kompromitteret, skal du straks kontakte dit pengeinstitut og lukke alle konti, der kan være blevet kompromitteret. Hold øje med eventuelle uforklarlige debiteringer på din konto.

Skift straks eventuelle adgangskoder, du måtte have afsløret. Hvis du brugte den samme adgangskode til flere ressourcer, skal du sørge for at ændre den for hver konto og ikke bruge den adgangskode i fremtiden.

4.1.5 Hvad er ondsindet kode?

Ondsindet kode er uønskede filer eller programmer, der kan forårsage skade på en computer eller kompromittere data, der er gemt på en computer. Forskellige klassifikationer af ondsindet kode omfatter vira, orme og trojanske heste.



Virus har evnen til at beskadige eller ødelægge filer på et computersystem og spredes ved at dele et allerede inficeret flytbart medie, åbne ondsindede vedhæftede filer og besøge ondsindede websider.

Orme er en type virus, der selv spreder sig fra computer til computer. Dens funktionalitet er at bruge alle din computers ressourcer, hvilket kan få din computer til at holde op med at reagere.

trojanske heste er computerprogrammer, der skjuler en virus eller et potentielt skadeligt program. Det er ikke ualmindeligt, at gratis software indeholder en trojansk hest, der får en bruger til at tro, at de bruger legitim software, i stedet udfører programmet ondsindede handlinger på din computer.

Ondsindede datafiler er ikke-eksekverbare filer – såsom et Microsoft Word-dokument, en Adobe PDF, en ZIP-fil eller en billedfil – der udnytter svagheder i det softwareprogram, der bruges til at åbne det. Angribere bruger ofte ondsindede datafiler til at installere malware på et offers system og distribuerer normalt filerne via e-mail, sociale medier og websteder.

Hvordan kommer du dig, hvis du bliver et offer for ondsindet kode?

Brug af antivirussoftware er den bedste måde at beskytte din computer mod skadelig kode. Hvis du tror, din computer er inficeret, skal du køre dit antivirusprogram. Ideelt set vil dit antivirusprogram identificere enhver ondsindet kode på din computer og sætte dem i karantæne, så de ikke længere påvirker dit system. Du bør også overveje disse yderligere trin:

- Minimer skaden. Hvis du er på arbejde og har adgang til en IT-afdeling, skal du kontakte dem med det samme. Jo før de kan undersøge og "rense" din computer, jo mindre sandsynligt er det, at det forårsager yderligere skade på din computer - og andre computere på netværket. Hvis du er på en hjemmecomputer eller bærbar computer, skal du frakoble din computer fra internettet; dette forhindrer hackeren i at få adgang til dit system.
- Fjern den ondsindede kode. Hvis du har antivirussoftware installeret på din computer, skal du opdatere softwaren og udføre en manuel scanning af hele dit system. Hvis du ikke har antivirussoftware, kan du købe det online eller i en computerbutik. Hvis softwaren ikke kan finde og fjerne infektionen, skal du muligvis geninstallere dit operativsystem, normalt med en systemgendannelsesdisk. Bemærk, at geninstallation eller gendannelse af operativsystemet typisk sletter alle dine filer og eventuel yderligere software, som du har installeret på din computer. Når du har geninstalleret operativsystemet og anden software, skal du installere alle de relevante patches for at rette kendte sårbarheder.

Trusler mod din computer vil fortsætte med at udvikle sig. Selvom du ikke kan eliminere enhver fare, kan du ved at udvise forsigtighed, installere og bruge antivirussoftware og følge andre simple sikkerhedsmetoder reducere din risiko betydeligt og styrke din beskyttelse mod ondsindet kode.

Hvad er sociale netværkssider?

Sociale netværkssider, nogle gange omtalt som "ven-af-en-ven"-websteder, bygger på konceptet med traditionelle sociale netværk, hvor du er forbundet med nye mennesker gennem mennesker, du allerede kender.

Formålet med nogle netværkssider kan være rent socialt, hvilket giver brugerne mulighed for at etablere venskaber eller romantiske forhold, mens andre kan fokusere på at etablere forretningsforbindelser.

Selvom funktionerne på sociale netværkssider er forskellige, giver de dig alle mulighed for at give oplysninger om dig selv og tilbyde en form for kommunikationsmekanisme (fora, chatrum, e-mail, onlinemeddelelser), der gør det muligt for dig at oprette forbindelse til andre brugere. På nogle sider kan du søge efter personer ud fra bestemte kriterier, mens andre sider kræver, at du bliver "introduceret" til nye mennesker gennem en forbindelse, du deler. Mange af webstederne har fællesskaber eller undergrupper, der kan være baseret på en bestemt interesse.

Hvilke sikkerhedsmæssige konsekvenser har disse websteder?

Sociale netværkssider er afhængige af forbindelser og kommunikation, så de opfordrer dig til at give en vis mængde personlige oplysninger. Når folk beslutter sig for, hvor meget information de skal afsløre, udviser folk muligvis ikke den samme grad af forsigtighed, som de ville, når de møder nogen personligt, fordi

- Internettet giver en følelse af anonymitet
- manglen på fysisk interaktion giver en falsk tryghed
- de skræddersyer oplysningerne, så deres venner kan læse dem, og glemmer, at andre kan se dem
- de ønsker at tilbyde indsigt for at imponere potentielle venner eller samarbejdspartnere

Selvom de fleste mennesker, der bruger disse websteder, ikke udgør en trussel, kan ondsindede personer blive tiltrukket af dem på grund af tilgængeligheden og mængden af personlige oplysninger, der er tilgængelige. Jo mere information ondsindede personer har om dig, jo lettere er det for dem at drage fordel af dig. Rovdyr kan danne relationer online og derefter overbevise intetanende personer om at møde dem personligt. Det kan føre til en farlig situation. De personlige oplysninger kan også bruges til at udføre et socialt ingeniørangreb. Ved at bruge oplysninger, du giver om din placering, hobbyer, interesser og venner, kan en ondsindet person efterligne en betroet ven eller overbevise dig om, at de har autoritet til at få adgang til andre personlige eller økonomiske data.

På grund af disse websteders popularitet kan angribere desuden bruge dem til at distribuere ondsindet kode. Websteder, der tilbyder applikationer udviklet af tredjeparter, er særligt modtagelige. Angribere kan muligvis oprette tilpassede programmer, der ser ud til at være uskyldige, mens de inficerer din computer eller deler dine oplysninger uden din viden.

4.1.6 Praktiske aktiviteter

Trin 1: Fjernelse af støv fra computere

1. Dette problem kan bemærkes af støjen, der produceres af køleventilatorernes hastighed, når du bruger den personlige computer eller den personlige bærbare computer.
2. Du har sikkert bemærket, at i begyndelsen af brugen af computeren, da den var ny, var køleventilatorerne stille, fordi køleventilatorerne ikke var støvede.
3. Efter længere tids brug bliver computeren/den bærbare computer meget støjende på grund af den høje hastighed på de støvede blæsere, som ikke længere formår at sikre den nødvendige luftstrøm for at afkøle de elektroniske komponenter i computeren, og når et punkt for at stoppe (lås) og fører til ødelæggelse af interne komponenter, mikroprocessorer på grund af den høje driftstemperatur.
4. Det negative aspekt ved støv er den termiske effekt, der skabes af aflejring af støv på komponenter (på og omkring processorens radiator).
5. Således kan tilstedeværelsen af støv i computeren forårsage ødelæggelse af elektroniske komponenter. På grund af støvet overophedes de, hvilket fører til deres ødelæggelse. Af denne grund skal computere støves jævnligt.
6. Hvis du antager, at du har en computer derhjemme, som du bruger, bedes du selv besvare følgende spørgsmål: "Hvornår var sidste gang, du rensede computeren for støv?"
7. Rengøring kan foretages på et specialiseret computerfejlfindingsværksted.
8. Støvrensning på bærbare computere kræver mere vanskelige operationer, derfor skal du ringe til en specialiseret service.
9. For at forstå, hvad det vil sige at rense en støvet computer, kan du søge på internettet, åbne en internetsøgemaskine og skrive i søgefeltet "hvordan renser du støv fra computere?". En hjemmeside vi anbefaler er:https://www.wikihow.com/Clean-a-Dusty-Computer
10. Men i betragtning af det faktum, at dette kursus henvender sig til begyndere, med mindre viden på dette område, anbefaler vi, at du for en start renser computeren for at bruge en specialiseret tjeneste.

COMPUTERS » COMPUTER MAINTENANCE

How to Clean a Dusty Computer

Co-authored by James Sears
Last Updated: October 15, 2020 References

Every computer slowly fills up with dust and other loose debris as it filters air through its hardware. While the goal of the fans found in any computer is to cool off all the components that get hot, the dust that clogs up a computer does the opposite. It's important to try and get rid of the dust in your computer with canned air and a microfiber cloth on a regular basis. However, a deeper clean with rubbing alcohol and cotton swabs might be necessary if it's been a while since your last dusting efforts.

Download Article

METHODS

1 Opening up Your Computer
2 Dusting Internal Components with Compressed Air
3 Deep Cleaning with Rubbing Alcohol
+ Show 1 more...

OTHER SECTIONS

Things You'll Need
Related Articles
References

Trin 2: For en computer er det nødvendigt at installere et antivirus/firewall-beskyttelsesprogram

1. For at forstå, hvad en antivirussoftware er, anbefaler vi, at du går ind på webstedet: https://us.norton.com/internetsecurity-malware-what-is-antivirus.html

2. Selvfølgelig er der mange antivirussoftware på markedet. En internetsøgning, for eksempel efter søgeordene "antivirus software sammenligne" kan finde utallige sider for at finde information om eksisterende software, såsom:https://www.pcmag.com/picks/the-best-antivirus-protection hvor der i afsnittet "VORES 13 TOP VALG" er opført flere antivirussoftware

3. Hvis du ikke har et andet antivirus installeret på din computer, anbefaler vi, at du søger på en søgeside efter søgeordene "gratis prøveversion antivirus" og får adgang til linkethttps://www.kaspersky.com/downloads/thank-you/antivirus-free-trial og på den åbnede side skal du klikke på knappen "DOWNLOAD NU".

4. Computeren vi bruger har eksempelvis WINDOWS 10 styresystem og "Google Chrome" som internetbrowser

5. Anbefalingen til Kaspersky blev lavet, på grund af det faktum, at det er antivirussikkerhedsløsningen installeret på den computer, vi bruger, og for ikke at skabe konflikter med andre typer antivirussoftware, anbefalede vi denne løsning.

6. I bunden af Chrome-browservinduet, efter at have trykket på knappen "DOWNLOAD NU", vises det eksekverbare arkiv "kav21.3.10.391en_26075.exe" (naturligvis kan arkivnavnet variere afhængigt af den downloadede version)

7. Nu efter at have downloadet fra internettet og installeret, har du installeret en antivirus-sikkerhedsløsning på din computer! Tillykke!

8. Antivirussen virker altid og er aktiv i baggrunden af operativsystemet

9. Nederst til højre på skærmen, ved siden af uret, vises et ikon med et "K". Det er muligt, at dette ikon er skjult af Windows-systemet, hvorfor det er nødvendigt først at klikke på knappen "^" ved siden af uret

10. Hvis du klikker på "K"-ikonet, åbnes grænsefladen til Kaspersky antivirus-indstillinger.

11. I den åbnede grænseflade skal du klikke på knappen "TASKS" og i det åbne vindue i "FULD SCAN"-området klikke på START. Vi bemærker, at antivirussoftwaren begynder at scanne computeren for virus, hvis der findes nogen.

12. Når scanningen er fuldført, kan scanningen genstartes, når det ønskes. Antivirus kan indstilles til at starte computerscanningsprocessen automatisk

13. Også i dette åbnede vindue, når du klikker på OPGAVER, scroller du nedenunder, kommer du til OPDATERING-området. Ved at trykke på START-knappen i dette område vil antivirusprogrammet blive opdateret til den seneste version og til den seneste database leveret af producenten. Det anbefales, at denne opdatering udføres med jævne mellemrum

14. Det skal bemærkes, at sikkerhedsløsninger både kan være til at beskytte din personlige computer mod virus og til at beskytte din computer mod uautoriseret adgang, når computeren er i et computernetværk.

15. For denne situation på webstedet for Kaspersky https://www.kaspersky.com/home-security præsenteres 3 varianter af beskyttelsessoftwaren, ved siden af hver er specificeret for, hvad den kan sikre beskyttelsen

16. For eksempel er beskyttelsesløsningen "Kaspersky Internet Security" en integreret løsning, der giver både antivirusbeskyttelse og beskyttelse i computernetværket (firewall).

17. Generelt tilbyder al antivirusbeskyttelsessoftware integrerede muligheder for både antivirusbeskyttelse og beskyttelse i computernetværket.

18. På samme måde kan andre antivirusprogrammer installeres ved at gå til producentens dedikerede side til download og køb af relaterede licenser.

19. Præsentationen er ikke strengt begrænset til Kaspersky antivirus! Når du vælger og i henhold til hver enkelt af jers behov, kan anden antivirussoftware på samme måde installeres både på computeren og på bærbare elektroniske systemer.

4.2 Beskyttelse af personlige data og privatliv

Enhed 4.2	Beskyttelse af personlige data og privatliv
Varighed	9 timer
Mål	At være opmærksom på problemer relateret til deling af personlige data For at kunne opsætte sikkerhedsindstillinger for at bevare privatlivets fred
Indhold	4.2.1 Beskyttelse af dig selv online 4.2.2 Retningslinjer for deling af personlige oplysninger 4.2.3 Praktiske aktiviteter
Ressourcer	Træningsmanual, computere med internetadgang
Træningsmetoder	Præsentation af træner Gruppeøvelse Diskussion / Debat

Bord 23- Kompetenceenhedens opbygning 4.2. – Beskyttelse af personlige data og privatlivets fred for Modul 4 – Sikkerhed.

4.2.1 Beskyt dig selv online

Hvordan kan du beskytte dig selv?

Begræns mængden af personlige oplysninger, du sender - Indsend ikke oplysninger, der ville gøre dig sårbar, såsom din adresse eller oplysninger om din tidsplan eller rutine. Hvis dine forbindelser sender oplysninger om dig, skal du sørge for, at de kombinerede oplysninger ikke er mere, end du ville være fortrolig med, at fremmede ved. Vær også hensynsfuld, når du poster oplysninger, herunder billeder, om dine forbindelser.

Husk, at internettet er en offentlig ressource - Indsend kun oplysninger, som du er tryg ved, at alle ser. Dette inkluderer oplysninger og billeder i din profil og i blogs og andre fora. Også, når du først har lagt oplysninger online, kan du ikke trække dem tilbage. Selvom du fjerner oplysningerne fra et websted, kan gemte eller cachelagrede versioner stadig eksistere på andres maskiner.

Vær på vagt over for fremmede - Internettet gør det nemt for folk at fordreje deres identiteter og motiver. Overvej at begrænse antallet af personer, der må kontakte dig på disse websteder. Hvis du interagerer med personer, du ikke kender, skal du være forsigtig med mængden af information, du afslører eller accepterer at møde dem personligt.

Vær skeptisk - Tro ikke på alt, hvad du læser på nettet. Folk kan sende falske eller vildledende oplysninger om forskellige emner, herunder deres egen identitet. Dette er ikke nødvendigvis gjort med ondsindet hensigt; det kan være utilsigtet, en overdrivelse eller en vittighed. Tag dog passende forholdsregler, og prøv at verificere ægtheden af enhver information, før du foretager dig noget.

Vurder dine indstillinger - Udnyt et websteds privatlivsindstillinger. Standardindstillingerne for nogle websteder kan tillade alle at se din profil, men du kan tilpasse dine indstillinger for kun at begrænse adgangen til bestemte personer. Der er stadig en risiko for, at private oplysninger kan blive afsløret på trods af disse begrænsninger, så lad være med at poste noget, som du ikke ønsker, at offentligheden skal se. Websteder kan ændre deres muligheder med jævne mellemrum, så gennemgå dine sikkerheds- og privatlivsindstillinger regelmæssigt for at sikre dig, at dine valg stadig er passende.

Vær på vagt over for tredjepartsapplikationer - Tredjepartsapplikationer kan levere underholdning eller funktionalitet, men vær forsigtig, når du beslutter, hvilke applikationer der skal aktiveres. Undgå applikationer, der virker mistænkelige, og modificer dine indstillinger for at begrænse mængden af information, applikationerne kan få adgang til.

Brug stærke adgangskoder - Beskyt din konto med adgangskoder, der ikke let kan gættes. Hvis din adgangskode er kompromitteret, kan en anden muligvis få adgang til din konto og udgive sig for at være dig.

Tjek privatlivspolitikker - Nogle websteder deler muligvis oplysninger såsom e-mailadresser eller brugerpræferencer med andre virksomheder. Dette kan føre til en stigning i spam. Prøv også at finde politikken for håndtering af henvisninger for at sikre, at du ikke utilsigtet tilmelder dine venner spam. Nogle websteder vil fortsætte med at sende e-mail-beskeder til alle, du henviser, indtil de tilmelder sig.

Hold software, især din webbrowser, opdateret - Installer softwareopdateringer, så angribere ikke kan drage fordel af kendte problemer eller sårbarheder. (Se Forstå patches.) Mange operativsystemer tilbyder automatiske opdateringer. Hvis denne mulighed er tilgængelig, skal du aktivere den.

Brug og vedligehold antivirussoftware - Antivirussoftware hjælper med at beskytte din computer mod kendte vira, så du kan muligvis opdage og fjerne virussen, før den kan gøre skade. (Se Forstå antivirussoftware.) Fordi angribere konstant skriver nye vira, er det vigtigt at holde dine definitioner ajour.

Børn er særligt modtagelige over for de trusler, som sociale netværkssider udgør- Selvom mange af disse websteder har aldersbegrænsninger, kan børn give forkerte oplysninger om deres alder, så de kan deltage. Ved at lære børn om internetsikkerhed, være opmærksomme på deres online-vaner og guide dem til passende websteder, kan forældre sikre, at børnene bliver sikre og ansvarlige brugere.

Hvorfor er det vigtigt at huske, at internettet er offentligt?

Internettet er en tilgængelig, populær ressource til at kommunikere med andre og udføre forskning. Du kan have en følelse af anonymitet, mens du er online, men bør huske, at du ikke er anonym, og det er lige så nemt for folk at finde information om dig, som det er for dig at finde information om dem.

Mange mennesker er blevet så fortrolige og fortrolige med internettet, at de anvender praksis, der gør dem sårbare. For eksempel, selvom folk typisk er forsigtige med at dele personlige oplysninger med fremmede, de møder på gaden, tøver de måske ikke med at lægge de samme oplysninger ud på nettet. Når først det er online, kan det tilgås af en verden af fremmede, og du aner ikke, hvad de kan gøre med den information.

4.2.2 Retningslinjer for deling af personlige oplysninger

Hvilke retningslinjer kan du følge, når du offentliggør information på internettet?

Se internettet som en roman, ikke en dagbog. Sørg for, at du er tryg ved, at alle kan se de oplysninger, du lægger på blogs, sociale netværkssider og personlige websteder – skriv det med en forventning om, at det er tilgængeligt til offentligt forbrug, og at folk, du aldrig har mødt, vil finde din side. Selvom nogle websteder bruger

adgangskoder eller andre sikkerhedsbegrænsninger til at beskytte oplysningerne, bruges disse metoder ikke til de fleste websteder. Hvis du ønsker, at oplysningerne skal være private eller begrænset til en lille, udvalgt gruppe mennesker, er internettet ikke det bedste forum.

Begræns mængden af personlige oplysninger, du sender. Post ikke oplysninger, der kan gøre dig sårbar, såsom din adresse, telefonnummer, e-mail eller oplysninger om din tidsplan eller rutine. Hvis du angiver din e-mail-adresse, kan det øge mængden af spam, du modtager (se Reduktion af spam for mere information). At give detaljer om dine hobbyer, dit job, din familie og venner eller din fortid kan give angribere nok information til at udføre et vellykket social engineering-angreb (se Undgå social engineering og phishing-angreb og forbliv sikker på sociale netværkssider for mere information).

Indse, at du ikke kan tage det tilbage. Når du først udgiver noget online, er det tilgængeligt for andre mennesker og for søgemaskiner. Du kan ændre eller fjerne oplysninger, efter at noget er blevet offentliggjort, men det er muligt, at nogen allerede har set den originale version. Selvom du forsøger at fjerne siden(erne) fra internettet, kan nogen have gemt en kopi af siden eller brugt uddrag i en anden kilde. Nogle søgemaskiner "cacherer" kopier af websider; disse cachelagrede kopier kan være tilgængelige, efter at en webside er blevet slettet eller ændret. Nogle webbrowsere kan også opretholde en cache af de websider, en bruger har besøgt, så den originale version kan blive gemt i en midlertidig fil på brugerens computer. Tænk over disse implikationer, før du udgiver oplysninger – når først noget er derude, kan du ikke garantere, at du helt kan fjerne det.

Som en generel praksis, lad din sunde fornuft styre dine beslutninger om, hvad du skal poste online. Før du udgiver noget på internettet, skal du bestemme, hvilken værdi det giver, og overveje konsekvenserne af at have informationen tilgængelig for offentligheden. Identitetstyveri er et stigende problem, og jo mere information en angriber kan indsamle om dig, jo lettere er det at udgive sig for at være dig.

Hvor anonym er du?

Du tror måske, at du er anonym, når du surfer på hjemmesider, men stykker information om dig bliver altid efterladt. Du kan reducere mængden af oplysninger, der afsløres om dig, ved at besøge legitime websteder, tjekke privatlivspolitikker og minimere mængden af personlige oplysninger, du giver.

Hvilke oplysninger indsamles?

Når du besøger et websted, sendes en vis mængde information automatisk til webstedet. Disse oplysninger kan omfatte følgende:

- IP-adresse - Hver computer på internettet er tildelt en specifik, unik IP-adresse (internetprotokol). Din computer kan have en statisk IP-adresse eller en dynamisk IP-adresse. Hvis du har en statisk IP-adresse, ændres den aldrig. Nogle internetudbydere ejer dog en blok af adresser og tildeler en åben, hver gang du opretter forbindelse til internettet - dette er en dynamisk IP-adresse. Du kan bestemme din computers IP-adresse til enhver tid ved at besøge www.showmyip.com.
- Domænenavn - Internettet er opdelt i domæner, og hver brugers konto er knyttet til et af disse domæner. Du kan identificere domænet ved at se i slutningen af URL; f.eks. angiver .edu en uddannelsesinstitution, .gov angiver et amerikansk regeringsorgan, .org henviser til organisation, og .com er til kommerciel brug. Mange lande har også specifikke domænenavne. Listen over aktive domænenavne er tilgængelig fra Internet Assigned Numbers Authority (IANA).
- Softwaredetaljer - Det kan være muligt for en organisation at bestemme, hvilken browser, inklusive den version, du brugte til at få adgang til dens websted. Organisationen kan muligvis også bestemme, hvilket operativsystem din computer kører.
- Sidebesøg - Information om hvilke sider du har besøgt, hvor længe du blev på en given side, og om du kom til siden fra en søgemaskine, er ofte tilgængelig for den organisation, der driver hjemmesiden.
- Hvis et websted bruger cookies, kan organisationen muligvis indsamle endnu flere oplysninger, såsom dine browsingmønstre, som omfatter andre websteder, du har besøgt. Hvis det websted, du besøger, er ondsindet, kan filer på din computer, såvel som adgangskoder, der er gemt i den midlertidige hukommelse, være i fare.

Hvordan bruges disse oplysninger?

Generelt bruger organisationer de oplysninger, der indsamles automatisk, til legitime formål, såsom at generere statistik om deres websteder. Ved at analysere statistikken kan organisationerne bedre forstå sidens popularitet, og hvilke indholdsområder der tilgås mest. De kan muligvis bruge disse oplysninger til at ændre webstedet for bedre at understøtte adfærden hos de personer, der besøger det.

En anden måde at anvende oplysninger indsamlet om brugere på er markedsføring. Hvis webstedet bruger cookies til at bestemme andre websteder eller sider, du har besøgt, kan det bruge disse oplysninger til at annoncere for bestemte produkter. Produkterne kan være på samme websted eller kan tilbydes af partnerwebsteder.

Nogle websteder kan dog indsamle dine oplysninger til ondsindede formål. Hvis angribere er i stand til at få adgang til filer, adgangskoder eller personlige oplysninger på din computer, kan de muligvis bruge disse data til deres fordel. Angriberne kan muligvis stjæle din identitet, bruge og misbruge dine personlige oplysninger til økonomisk vinding. En almindelig praksis er, at angribere bruger denne type information en eller to gange og derefter sælger eller bytter dem til andre mennesker. Angriberne tjener på salget eller handelen, og en stigning i antallet af transaktioner gør det sværere at spore enhver aktivitet tilbage til dem. Angriberne kan også ændre sikkerhedsindstillingerne på din computer, så de kan få adgang til og bruge din computer til anden ondsindet aktivitet.

Afslører du andre personlige oplysninger?

Selvom brug af cookies kan være en metode til at indsamle oplysninger, er den nemmeste måde for angribere at få adgang til personlige oplysninger på at bede om dem. Ved at repræsentere et ondsindet websted som et legitimt, kan angribere muligvis overbevise dig om at give dem din adresse, kreditkortoplysninger, cpr-nummer eller andre personlige data.

4.2.3 Praktiske aktiviteter

Trin 1: Lås computeren med adgangskode

1. Dagens udstyr tilbyder flere måder at beskytte dig selv på! For eksempel i WINDOWS 10 i sektionen INDSTILLINGER -> Loginindstillinger har du mulighed for at give din computer adgangskode gennem en af mulighederne: ansigtsgenkendelse, fingeraftryk, pinkode, sikkerhedsnøgle, adgangskode eller billedgenkendelse.
2. Vi vil ikke diskutere alt dette i dag, men det skal nævnes, at enhver computer tilbyder muligheden for at indstille en adgangskode (dette kan gøres generelt fra afsnittet INDSTILLINGER på dit udstyr)
3. I dag fokuserer vi på at sætte en adgangskode. Adgangskoden er en sekvens af tegn skrevet i en given rækkefølge, som kan indeholde: store bogstaver, små bogstaver, tal, specialtegn
4. For eksempel, hvis vi i WINDOWS indstiller adgangskoden "@calculatorMeuDeNota10" til INDSTILLINGER -> Log-in muligheder, så vil adgangskoden blive anmodet om, når du får adgang til computeren ved genstart eller afslutter operativsystemet fra standby. Hvilken adgangskode? @calculatorulMeuDeNota10, bogstaverne skrevet i nøjagtig samme rækkefølge og samme type bogstav.

BEMÆRK: computeren vil ikke genkende adgangskoden @CALCULATORULMEUDENOTA10 eller @calculatorulmeudenota10 eller @ calculatorulMeu De Nota 10. Adgangskoden, der genkendes af systemet, vil være nøjagtig som den etablerede, henholdsvis @ calculatorulMeuDeNota10

5. OBS: et sæt kodeord, glem det ikke! Det ville være bedst at skrive det ned et sted, hvor du kan finde det. Hvis du har glemt din adgangskode, er der forskellige måder at gendanne den på, men dette kræver meget mere avanceret viden og giver ofte problemer med at gendanne den.
6. En adgangskode skal indeholde specialtegn (@), små bogstaver (computer eu e ota), store bogstaver (MDN), tal (10).
7. Jo flere tegn en adgangskode indeholder, den adgangskode vil være meget stærkere, og det vil være sværere for nogen at finde den.
8. For at forstå, hvad en stærk adgangskode er, anbefaler vi, at du går ind på følgende websted:https://ro.safetydetectives.com/password-meter/
9. I øverste højre del kan du indstille det sprog, som oplysningerne fra siden skal vises på
10. I feltet under overskriften "Hvor sikker er min adgangskode?" du kan indtaste og teste adgangskodemønstre
11. Jo højere antal tegn adgangskoden indeholder og flere karakterer anført ovenfor, jo højere score opnås i højre side af feltet, og adgangskodens type bliver fra MEGET SVAG til MEGET STÆRK
12. Prøv at finde en adgangskode, der får karakteren 100! Lykkes det? Adgangskode fra denne øvelse, hvilken score tror du, den får?
13. Til sidst anbefaler vi, at du læser afsnittet Ofte stillede spørgsmål nederst på sidenhttps://ro.safetydetectives.com/password-meter/
14. På denne måde får du mere information om, hvordan du laver rigtig gode og sikre adgangskoder.

Trin 2: Brug af en browser og periodiske opdateringer

1. Åbn en webside, skriv internetadressen www.google.com og skriv følgende ord "chrome download" i søgefeltet
2. På computeren skal du søge efter og downloade Chrome-internetbrowseren (hvis den ikke allerede er installeret) påhttps://www.google.com/chrome/
3. Fra den åbnede side skal du trykke på knappen DOWNLOAD CHROME
4. Få adgang til den downloadede fil, og følg installationstrinnene
5. Åbn en eller flere websider i Chrome-browseren (det er op til dig, hvilke websider du vil have adgang til)
6. Bemærk i navigationslinjen, hvorvidt der er en hængelås foran den tilgåede internetadresse

7. Denne hængelås repræsenterer et sikkerhedscertifikat for den tilgåede side, og i dens fravær er navigationen på siden ikke sikker. Så en sikker browsing kan foretages på de internetsider, når hængelåsen eksisterer
8. På en sikker webside (hvor den hængelås findes), skal du klikke på den hængelås og se ud fra de angivne oplysninger, om certifikatet er gyldigt
9. Klik på Certifikat (Gyldigt) og hold øje med den dato, hvor certifikatet er gyldigt
10. "Låse"-ikonet er en bekræftelse på, at internetforbindelsen mellem den person, der får adgang til dette websted og serveren på det websted, er en sikker forbindelse, det er en krypteret kommunikation (andre brugere kan ikke få adgang til, opsnappe, din etablerede forbindelse med den internet side)
11. Luk vinduet med certifikatoplysninger, og klik på de 3 lodrette prikker øverst til højre (placeret under X-luk-vinduet) for at få adgang til Chrome-indstillinger
12. Klik på "Hjælp" og i den nye menu klik på "Om Google Chrome"
13. På dette tidspunkt vil Google Chrome forsøge at opdatere til den seneste tilgængelige version af softwaren med følgende meddelelse:
    "Opdaterer Google Chrome (50%)
    Version 90.0.4430.212 (officiel bygning) (64-bit)"
14. Efter opdateringen kan Chrome bede dig om at genstarte din browser med en besked
    "Næsten up to date! Genstart Google Chrome for at afslutte opdateringen. Inkognitovinduer åbnes ikke igen.
    Version 90.0.4430.212 (officiel bygning) (64-bit)"
15. Tryk på knappen "Genstart"
16. Hvis det ikke er nødvendigt at genåbne browseren, eller browseren allerede er opdateret, vises en meddelelse
    "Google Chrome er opdateret
    Version 91.0.4472.77 (officiel bygning) (64-bit)"
17. På denne måde kan Chrome-browseren opdateres
18. Bemærk venligst, at enhver software og ikke kun Chrome-browseren giver mulighed for at opdatere til højere versioner, men ikke al software tilbyder denne funktion gratis
19. Opdatering til nyere versioner giver sikkerheden og stabiliteten af den software, der bruges

4.3 Beskyttelse af sundhed og velvære

Enhed 4.3	Beskyttelse af sundhed og velvære
Varighed	5 timer
Mål	at være i stand til at undgå sundhedsrisici og trusler mod fysisk og psykisk velvære ved brug af digitale teknologier; at kunne beskytte sig selv og andre mod mulige farer i digitale miljøer; at være i stand til at kontrollere de aspekter, der distraherer fra arbejde og det digitale liv; at kunne træffe forebyggende foranstaltninger for at beskytte sundheden for den person, han har ansvaret for
Indhold	4.3.1 Negative virkninger af teknologi: hvad skal man vide 4.3.2 Har du hørt om cybermobning? 4.3.3 Praktiske aktiviteter
Ressourcer	Træningsmanual, computere med internetadgang
Træningsmetoder	Præsentation af træner

Bord 24- Kompetenceenhedens opbygning 4.3. – Beskyttelse af sundhed og velvære i Modul 4 – Sikkerhed.

4.3.1 Negative virkninger af teknologi: hvad man skal vide

Folk er mere forbundet end nogensinde, i høj grad takket være hurtige fremskridt inden for teknologi.

Mens nogle former for teknologi kan have foretaget positive ændringer i verden, er der også beviser for de negative virkninger af teknologi og dens overforbrug.

Sociale medier og mobile enheder kan føre til psykiske og fysiske problemer, såsom øjenbelastning og vanskeligheder med at fokusere på vigtige opgaver. De kan også bidrage til mere alvorlige helbredstilstande, såsom depression.

Psykologiske effekter

Overforbrug eller afhængighed af teknologi kan have negative psykologiske virkninger, herunder: Isolation. Teknologier, såsom sociale medier, er designet til at bringe mennesker sammen, men alligevel kan de have den modsatte effekt i nogle tilfælde.

En undersøgelse fra 2017 af unge voksne i alderen 19-32 år viste, at personer med større brug af sociale medier var mere end tre gange så tilbøjelige til at føle sig socialt isolerede end dem, der ikke brugte sociale medier så ofte.

At finde måder at reducere brugen af sociale medier på, såsom at sætte tidsgrænser for sociale apps, kan hjælpe med at reducere følelsen af isolation hos nogle mennesker.

Depression og angst

Forfatterne af en systematisk gennemgang fra 2016, Trusted Source, diskuterede sammenhængen mellem sociale netværk og mentale sundhedsproblemer, såsom depression og angst.

Deres forskning fandt blandede resultater. Folk, der havde mere positive interaktioner og social støtte på disse platforme, så ud til at have lavere niveauer af depression og angst.

Det omvendte var dog også sandt. Folk, der opfattede, at de havde flere negative sociale interaktioner online, og som var mere tilbøjelige til social sammenligning, oplevede højere niveauer af depression og angst.

Så selvom der ser ud til at være en forbindelse mellem sociale medier og mental sundhed, er en væsentlig afgørende faktor, hvilke typer interaktioner folk føler, de har på disse platforme.

Fysiske sundhedseffekter

Teknologibrug kan også øge risikoen for fysiske problemer, herunder:

Øjenspænding

Teknologier, såsom håndholdte tablets, smartphones og computere, kan fastholde en persons opmærksomhed i lange perioder. Dette kan føre til anstrengte øjne.

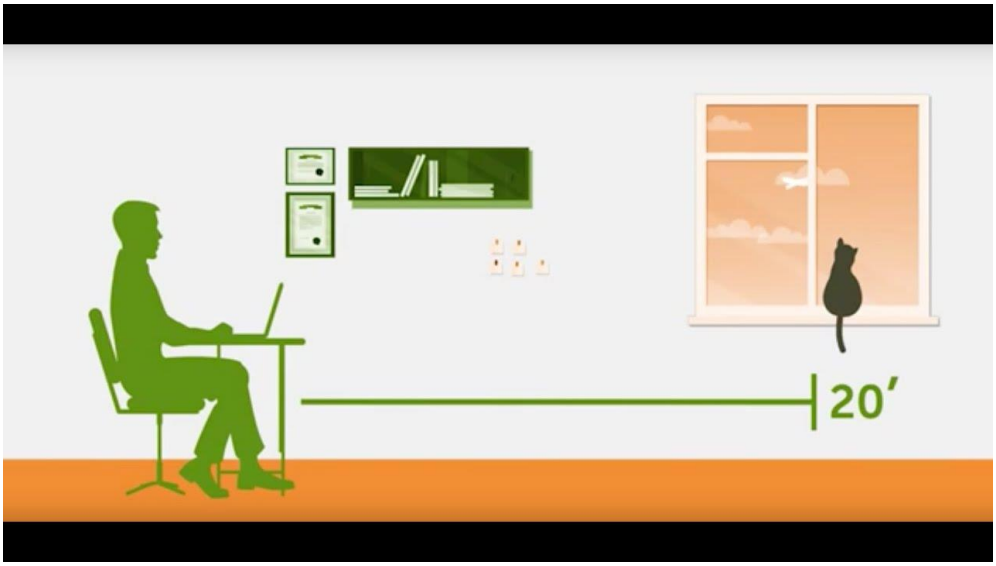
Symptomer på digital øjenbelastning kan omfatte sløret syn og tørre øjne. Øjenbelastning kan også føre til smerter i andre områder af kroppen, såsom hoved, nakke eller skuldre.

Flere teknologiske faktorer kan føre til anstrengte øjne, såsom:

- skærmtid
- blænding på skærmen
- skærmens lysstyrke
- ser for tæt på eller for langt væk
- dårlig siddestilling
- underliggende synsproblemer

Regelmæssige pauser væk fra skærmen kan reducere sandsynligheden for anstrengte øjne.

Enhver, der regelmæssigt oplever disse symptomer, bør se en optometrist til kontrol.



20-20-20-reglen for digital visning

Når du bruger enhver form for digital skærm i længere tid, anbefales det at bruge 20-20-20-reglen. For at bruge reglen skal du efter hvert 20. minuts skærmtid tage en 20-sekunders pause for at se på noget, der er mindst 20 m væk. At gøre dette kan hjælpe med at reducere belastningen af øjnene fra at stirre på en skærm i en sammenhængende periode.

Dårlig holdning

Den måde, mange mennesker bruger mobile enheder og computere på, kan også bidrage til forkert kropsholdning. Over tid kan dette føre til muskuloskeletale problemer. Mange teknologier fremmer en "ned og frem" brugerposition, hvilket betyder, at personen er bøjet fremad og kigger ned på skærmen. Dette kan lægge et unødigt stort pres på nakke og rygsøjle. En 5-årig undersøgelse i tidsskriftet Applied Ergonomics fandt en sammenhæng mellem sms'er på en mobiltelefon og nakke- eller øvre rygsmerter hos unge voksne. Resultaterne indikerede, at virkningerne for det meste var kortvarige, selvom nogle mennesker fortsatte med langvarige symptomer.

Nogle undersøgelser udfordrer dog disse resultater.

En undersøgelse fra 2018, Trusted Source i European Spine Journal, fandt ud af, at halsens stilling, mens du sms'er, ikke gjorde nogen forskel i symptomer som nakkesmerter.

Denne undersøgelse konkluderede, at sms og "tekst-nakke" ikke påvirkede nakkesmerter hos unge voksne. Undersøgelsen omfattede dog ikke en langtidsopfølgning. Det kan være, at andre faktorer også påvirker nakkesmerter, såsom alder og aktivitetsniveau. At rette holdningsproblemer, mens du bruger teknologi, kan føre til en generel forbedring af kropsholdning og styrke i kerne, nakke og ryg.

For eksempel, hvis en person finder sig selv at sidde i samme stilling i timevis ad gangen, såsom at sidde ved et skrivebord, mens han arbejder, kan regelmæssig stående eller strække sig hjælpe med at reducere belastningen på kroppen.

Derudover kan korte pauser, såsom at gå rundt på kontoret hver time, også hjælpe med at holde musklerne løse og undgå spændinger og forkert holdning.

Søvnproblemer

Brug af teknologi for tæt på sengetid kan give problemer med søvnen. Denne effekt har at gøre med, at blåt lys, såsom lyset fra mobiltelefoner, e-læsere og computere, stimulerer hjernen. Forfattere af en undersøgelse fra 2014 fandt ud af, at dette blå lys er nok til at forstyrre kroppens naturlige døgnrytme. Denne forstyrrelse kan gøre det sværere at falde i søvn eller føre til, at en person føler sig mindre opmærksom den næste dag. For at undgå den potentielle indvirkning af blåt lys på hjernen, kan folk stoppe med at bruge elektroniske enheder, der udsender blåt lys i timen eller to før sengetid. Blide aktiviteter at slappe af med i stedet, såsom at læse en bog, lave blide stræk eller tage et bad, er alternativer.

Nedsat fysisk aktivitet

De fleste dagligdags digitale teknologier er stillesiddende. Mere udvidet brug af disse teknologier fremmer en mere stillesiddende livsstil, som er kendt for at have negative helbredseffekter, såsom at bidrage til:

- fedme
- kardiovaskulær sygdom
- type 2 diabetes
- for tidlig død

At finde måder at tage pauser fra stillesiddende teknologier kan hjælpe med at fremme en mere aktiv livsstil.

Forskning fra 2017 viser, at aktive teknologier, såsom app-notifikationer, e-mails og bærbare teknologier, der fremmer træning, kan reducere kortvarig stillesiddende adfærd. Dette kan hjælpe folk med at sætte sunde mønstre og blive mere fysisk aktive.

4.3.2 Har du hørt om cybermobning?

Cybermobning er at bruge teknologi til at chikanere eller mobbe en anden. Mobbere plejede at være begrænset til metoder som fysisk intimidering, post eller telefon, men computere, mobiltelefoner, tablets og andre mobile enheder tilbyder mobberfora såsom e-mail, onlinemeddelelser, websider og digitale billeder.

Former for cybermobning kan variere i sværhedsgrad fra grusomme eller pinlige rygter til trusler, chikane eller stalking. Det kan påvirke enhver aldersgruppe; dog er teenagere og unge voksne almindelige ofre, og cybermobning er et voksende problem i skolerne.

Hvorfor er cybermobning blevet sådan et problem?

Internettets relative anonymitet er tiltalende for bøller, fordi det øger intimideringen og gør det sværere at spore aktiviteten. Nogle bøller har også nemmere ved at være mere ondskabsfulde, fordi der ikke er nogen personlig kontakt. Internettet og e-mail kan også øge synligheden af aktiviteten. Oplysninger eller billeder, der er lagt online eller videresendt i masse-e-mails, kan nå ud til et større publikum hurtigere end mere traditionelle metoder, hvilket forårsager mere skade på ofrene. En stor mængde personlige oplysninger er tilgængelige online, så mobberne kan muligvis vælge deres ofre vilkårligt.

Cybermobning kan også indikere en tendens til mere seriøs adfærd. Mens mobning altid har været en uheldig realitet, vokser de fleste mobbere ud af det. Cybermobning har ikke eksisteret længe nok til at have solid forskning, men der er dokumentation for, at det kan være et tidligt varsel om voldelig adfærd.

Hvordan kan du beskytte dig selv eller dine børn?

- Lær dine børn gode onlinevaner. Forklar risiciene ved teknologi, og lær børn at være ansvarlige online. Reducer deres risiko for at blive cybermobbere ved at opstille retningslinjer for og overvåge deres brug af internettet og andre elektroniske medier (mobiltelefoner, tablets osv.).

- Hold kommunikationslinjer åbne. Tal jævnligt med dine børn om deres onlineaktiviteter, så de føler sig trygge ved at fortælle dig, hvis de bliver ofre.
- Hold øje med advarselsskilte. Hvis du bemærker ændringer i dit barns adfærd, så prøv at identificere årsagen så hurtigt som muligt. Hvis cybermobning er involveret, kan en tidlig handling begrænse skaden.
- Begræns tilgængeligheden af personlige oplysninger. Begrænsning af antallet af personer, der har adgang til kontaktoplysninger eller detaljer om interesser, vaner eller beskæftigelse, reducerer eksponeringen for mobbere, som du eller dit barn ikke kender. Dette kan begrænse risikoen for at blive et offer og kan gøre det lettere at identificere mobberen, hvis du eller dit barn bliver ofre.
- Undgå at eskalere situationen. At reagere med fjendtlighed vil sandsynligvis provokere en bølle og eskalere situationen. Afhængigt af omstændighederne kan du overveje at ignorere problemet. Ofte trives mobberne med reaktionen fra deres ofre. Andre muligheder omfatter subtile handlinger. For eksempel kan du muligvis blokere meddelelserne på sociale netværkssider eller stoppe uønskede e-mails ved at ændre e-mailadressen. Hvis du fortsætter med at få beskeder på den nye e-mailadresse, har du muligvis stærkere argumenter for retslige skridt.
- Dokumenter aktiviteten. Hold en fortegnelse over enhver online aktivitet (e-mails, websider, onlinemeddelelser osv.), herunder relevante datoer og tidspunkter. Ud over at arkivere en elektronisk version, kan du overveje at udskrive en kopi.
- Rapporter cybermobning til de relevante myndigheder. Hvis du eller dit barn bliver chikaneret eller truet, skal du rapportere aktiviteten. Mange skoler har indført programmer mod mobning, så skolens embedsmænd kan have etableret politikker for håndtering af aktiviteter, der involverer elever. Kontakt om nødvendigt din lokale retshåndhævelse.

4.3.3 Praktiske aktiviteter

Trin 1: Øjenbeskyttelse

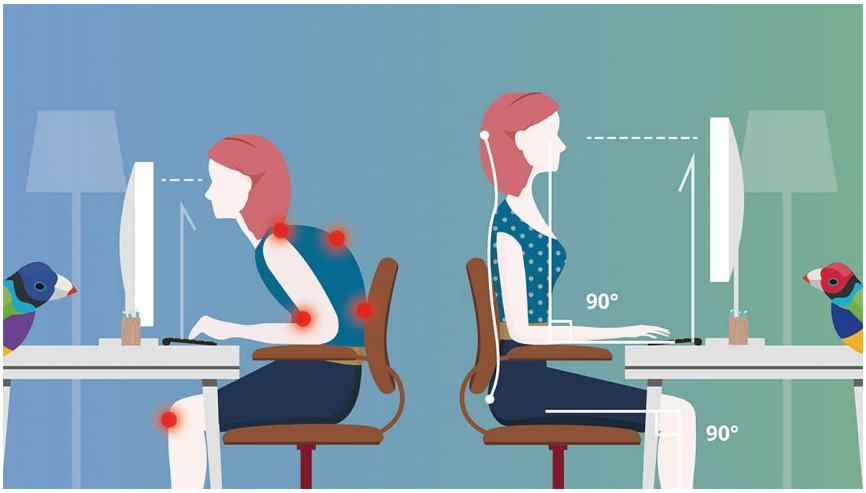
1. Åbn et MS Office- eller Notepad-redigeringsprogram på din computer. Vi brugte Notepad, en software inkluderet i Windows-operativsystemet.
2. Skriv en tekst på nogle få bogstaver/ord, med standard defineret skriftstørrelse uden at blive ændret.
3. Vælg med musen, teksten skrevet i Notesblok og med den valgte tekst, fra den øverste menulinje tryk Format-> Skrifttype-> og i området kaldet Størrelse vælges den største tilgængelige størrelse (i mit tilfælde 72). Læg mærke til, hvor let det er at læse den skrevne tekst, den afslappende følelse du har, når du læser en tekst med en større skriftstørrelse.
4. Vælg igen med musen, teksten skrevet i Notesblok og med den valgte tekst, fra den øverste menulinje tryk Format-> Skrifttype-> og i området kaldet Størrelse vælges den mindste størrelse, der er tilgængelig

for skrifttypen (i mit tilfælde 8). Læg mærke til øjet, hvor hårdt kan læse den skrevne tekst, følelsen af at tvinge øjet, som du føler, når du læser en tekst med en meget lille skriftstørrelse.

5. Hvis du vil observere disse 2 forskelle, kan du lave denne øvelse flere gange.
6. Se venligst på denne øvelse fra følgende perspektiv: Antag, at du bruger 5 timer om dagen foran computeren. Uanset om du har arbejde at lave, om du ser en film eller ser på billeder, vil øjet til enhver tid forsøge at tilpasse sig så meget og så godt som muligt for at læse så meget information fra billederne, der vises på skærmen, selvom at informationen er lettere eller sværere at se. Denne måde at tvinge øjet på kan føre til synsproblemer over tid.
7. Af denne grund er der forskellige måder at forlænge dit øjensundhed på. Google kender til dette problem og i udvidelserne i Google Chrome kan tilføjes en udvidelse suggestivt kaldet "eyeCare - Protect your vision". Det kan søges i google-søgemaskinen med nøgleord som "Eye Care Chrome" og fra de viste resultater få adgang til linkethttps://chrome.google.com/webstore/detail/eyecare-protect-your-visi/eeeningnfkaonkonalpcicgemnnijjhn
8. På siden ved siden af eyeCare - Beskyt din synsudvidelse skal du klikke på knappen "Tilføj til Chrome"
9. Klik på knappen Tilføj udvidelse i det nyligt åbnede vindue
10. Denne forlængelse er en rest for 20-20-20-reglen (hver 20. minut, tag øjnene fra din computer og se på noget 20 fod væk i mindst 20 sekunder)
11. På denne måde er øjet indstillet til at se på en anden afstand fra monitoren (20 fod væk), hvilket bidrager til øjets sundhed.

Trin 2: Beskyttelse af fysisk sundhed (computerarbejdsstilling)

1. Første trin i denne øvelse er at være opmærksom på den position du har foran computeren (ændr ikke denne position, stræk ikke ryggen. Bliv præcis i den position du er i, til næste punkt).
2. Se på billedet nedenfor, og sig, hvilken position du er i: venstre position (med rygsøjlen i en buet position) eller højre position (med højre rygsøjle)?



3. Så hvis du er i positionen på billedet til højre: TILLYKKE! Men hvis du er i den position på billedet til venstre, en position hvor de fleste mennesker normalt er, så skal du forstå følgende aspekter:
4. Efter en længere periode tilbragt foran elektronisk udstyr, ufrivilligt, uden at være klar over det, har kroppen en tendens til at slappe af, og fra den korrekte arbejdsstilling kan du nå positionen til venstre for billedet, hvilket med tiden fører til helbredsproblemer på rygsøjlen, især hos de mennesker, der bruger mange timer om dagen, og mange dage om ugen ved computeren
5. Af denne grund skal vi være opmærksomme på vores position, når vi arbejder på computeren og rette os selv! Denne lille indsats kan holde vores rygsøjle sund over tid.
6. Hvordan er din ryg nu? Har du rettet din rygsøjle?

4.4 Beskyttelse af miljøet

Enhed 4.4	Beskyttelse af miljøet
Varighed	5 timer
Mål	At kunne vælge sikre, effektive og omkostningseffektive medier At forstå digitale mediers indflydelse At vide, hvordan man bortskaffer elektroniske enheder sikkert
Indhold	4.4.1 Korrekt bortskaffelse af elektronisk udstyr 4.4.2 Praktiske aktiviteter

Ressourcer	Træningsmanual, computere med internetadgang
Træningsmetoder	Præsentation af træner Gruppeøvelse Diskussion / Debat

Bord 25- Kompetenceenhedens opbygning 4.4. – Beskyttelse af miljøet i Modul 4 – Sikkerhed.

4.4.1 Korrekt bortskaffelse af elektroniske enheder

Hvorfor er det vigtigt at bortskaffe elektroniske enheder på en sikker måde?

Ud over effektivt at sikre følsomme oplysninger på elektroniske enheder, er det vigtigt at følge bedste praksis for bortskaffelse af elektroniske enheder. Computere, smartphones og kameraer giver dig mulighed for at have en masse information lige ved hånden, men når du bortskaffer, donerer eller genbruger en enhed, kan du utilsigtet afsløre følsomme oplysninger, som kan blive udnyttet af cyberkriminelle.

Typer af elektroniske enheder omfatter:

- Computere, smartphones og tablets — elektroniske enheder, der automatisk kan lagre og behandle data; de fleste indeholder en central behandlingsenhed og hukommelse og bruger et operativsystem, der kører programmer og applikationer;
- Digitale medier - disse elektroniske enheder skaber, lagrer og afspiller digitalt indhold. Digitale medieenheder omfatter elementer som digitale kameraer og medieafspillere;
- Ekstern hardware og perifere enheder — hardwareenheder, der giver input og output til computere, såsom printere, skærme og eksterne harddiske; disse enheder indeholder permanent lagrede digitale tegn; og
- Spillekonsoller - elektroniske, digitale eller computerenheder, der udsender et videosignal eller et visuelt billede for at vise et videospil.

Hvad er nogle effektive metoder til at fjerne data fra din enhed?

Der er en række forskellige metoder til permanent at slette data fra dine enheder (også kaldet desinficering). Da metoderne til desinficering varierer alt efter enhed, er det vigtigt at bruge den metode, der gælder for den pågældende enhed.

Før du renser en enhed, bør du overveje at sikkerhedskopiere dine data. At gemme dine data på en anden enhed eller en anden placering (f.eks. en ekstern harddisk eller skyen) kan hjælpe dig med at gendanne dine data, hvis du ved et uheld sletter oplysninger, som du ikke havde til hensigt, eller hvis din enhed bliver stjålet (dette kan også hjælpe dig med at identificere præcis hvilke oplysninger en tyv kan have været i stand til at få adgang til). Muligheder for digital lagring omfatter cloud-datatjenester, cd'er, dvd'er og flytbare flashdrev eller flytbare harddiske.

Metoder til desinficering omfatter:

- Sletning af data. Fjernelse af data fra din enhed kan være en metode til desinficering. Når du sletter filer fra en enhed – selvom filerne kan se ud til at være blevet fjernet – forbliver data på mediet, selv efter at en slette- eller formateringskommando er udført. Stol ikke udelukkende på den slettemetode, du rutinemæssigt bruger, såsom at flytte en fil til papirkurven eller papirkurven eller vælge "slet" i menuen. Selvom du tømmer papirkurven, er de slettede filer stadig på enheden og kan hentes. Permanent sletning af data kræver flere trin.
- Computere. Brug en diskrensningssoftware designet til permanent at fjerne de data, der er gemt på en computers harddisk for at forhindre muligheden for gendannelse.
- Sikker sletning. Dette er et sæt kommandoer i firmwaren på de fleste computerharddiske. Hvis du vælger et program, der kører kommandosættet for sikker sletning, vil det slette dataene ved at overskrive alle områder på harddisken.

- Disk aftørring. Dette er et værktøj, der sletter følsomme oplysninger på harddiske og sikkert tørrer flashdrev og sikre digitale kort.
- Smartphones og tablets. Sørg for, at alle data er fjernet fra din enhed ved at udføre en "hård nulstilling". Dette vil returnere enheden til dens oprindelige fabriksindstillinger. Hver enhed har en anden hård nulstillingsprocedure, men de fleste smartphones og tablets kan nulstilles gennem deres indstillinger. Derudover skal du fysisk fjerne hukommelseskortet og abonnentidentitetsmodulkortet, hvis din enhed har et.
- Digitalkameraer, medieafspillere og spillekonsoller. Udfør en standard fabriksnulstilling (dvs. en hård nulstilling) og fjern fysisk harddisken eller hukommelseskortet.
- Kontorudstyr (f.eks. kopimaskiner, printere, faxmaskiner, multifunktionsenheder). Fjern eventuelle hukommelseskort fra udstyret. Udfør en fuld fremstillingsnulstilling for at gendanne udstyret til dets fabriksindstillinger.
- Overskrivning. En anden metode til desinficering er at slette følsomme oplysninger og skrive nye binære data over dem. Brug af tilfældige data i stedet for let identificerbare mønstre gør det sværere for angribere at opdage den originale information nedenunder. Da data, der er gemt på en computer, er skrevet i binær kode - strenge med 0'er og 1'ere - er en metode til at overskrive at nulfylde en harddisk og vælge programmer, der bruger alle nuller i det sidste lag. Brugere bør overskrive hele harddisken og tilføje flere lag af nye data (tre til syv gennemløb af nye binære data) for at forhindre angribere i at få de originale data.
- Cipher.exe er et indbygget kommandolinjeværktøj i Microsoft Windows-operativsystemer, der kan bruges til at kryptere eller dekryptere data på New Technology File System-drev. Dette værktøj sletter også sikkert data ved at overskrive det.
- Rydning er et niveau af medie-sanering, der ikke tillader, at oplysninger kan hentes af data-, disk- eller filgendannelsesværktøjer. Enheder skal være modstandsdygtige over for forsøg på gendannelse af tastetryk fra standardinputenheder (f.eks. et tastatur eller en mus) og fra dataopfangningsværktøjer.
- Ødelæggende. Fysisk ødelæggelse af en enhed er den ultimative måde at forhindre andre i at hente dine oplysninger. Specialiserede tjenester er tilgængelige, som vil desintegrere, brænde, smelte eller pulverisere dit computerdrev og andre enheder. Disse desinficeringsmetoder er designet til fuldstændigt at ødelægge mediet og udføres typisk på en outsourcet metaldestruktion eller et licenseret forbrændingsanlæg. Hvis du vælger ikke at bruge en tjeneste, kan du ødelægge din harddisk ved selv at slå søm eller bore huller i enheden. De resterende fysiske dele af drevet skal være små nok (mindst 1/125 tommer), til at dine oplysninger ikke kan rekonstrueres ud fra dem. Der er også tilgængelige hardwareenheder, som sletter cd'er og dvd'er ved at ødelægge deres overflade.
- Magnetiske medieafgassere. Degaussere udsætter enheder for stærke magnetiske felter, der fjerner de data, der er magnetisk lagret på traditionelle magnetiske medier.

- Fast-state ødelæggelse. Ødelæggelsen af al datalagerchiphukommelse ved at knuse, makulere eller desintegration kaldes solid-state destruktion. Solid State-drev bør destrueres med enheder, der er specielt udviklet til dette formål.
- Destruktion af cd og dvd. Mange kontor- og hjemmemakuleringsmaskiner kan makulere cd'er og dvd'er (sørg for at kontrollere, at makuleringsmaskinen, du bruger, kan makulere cd'er og dvd'er, før du forsøger denne metode).

Hvordan kan du sikkert bortskaffe forældede elektroniske enheder?

Elektronisk affald (nogle gange kaldet e-affald) er et udtryk, der bruges til at beskrive elektronik, der nærmer sig slutningen af deres levetid og kasseres, doneres eller genbruges. Selvom donation og genbrug af elektroniske enheder skåner naturressourcerne, kan du stadig vælge at bortskaffe e-affald ved at kontakte din lokale losseplads og anmode om et udpeget afleveringssted for e-affald. Vær opmærksom på, at selvom der er mange muligheder for bortskaffelse, er det dit ansvar at sikre, at det valgte sted er velrenommeret og certificeret.

4.4.2 Praktiske aktiviteter

Trin 1: Elforbrug - Driftsomkostninger for udstyr

1. Som vi alle kender elektrisk udstyr, kan det kun fungere, hvis det er drevet af elektricitet. Men hvor meget energi forbruges en computer? For at få svaret, lad os gennemgå beregningen beskrevet nedenfor.

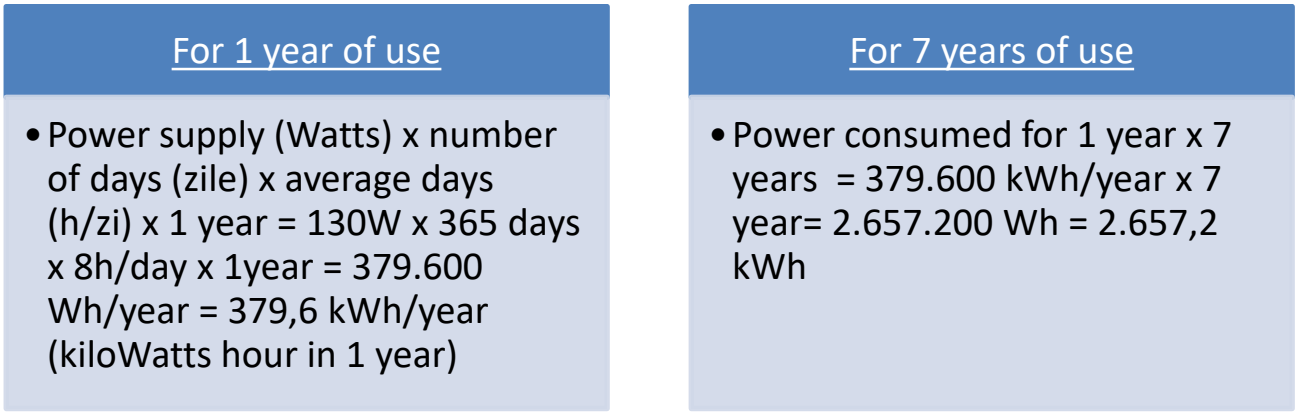
2. Overvej to computerenheder: en bærbar (for eksempel den, jeg bruger) og en computer (en central enhed), med tekniske egenskaber, der er omtrent de samme som den bærbare computer

3. Laptop: Jeg læste værdien af strømforsyningen til den bærbare computer, og jeg bemærker, at den er 130W (watt)

4. Lad os sammen lave følgende beregning: bærbar brugt 7 dage om ugen (5 dage på arbejde og 2 dage i weekenden til film, musik, fotos osv.), omkring 8 timer/dag (t/dag) i gennemsnit

5. Lad os anslå den gennemsnitlige levetid for den bærbare computer til omkring 5 til 7 år

6. Lad os beregne strømforbruget for denne bærbare computer som følger:



Figur 12 – Data til beregning af strømforbruget.

7. Computerberegning (central enhed): Vi lavede en undersøgelse på internettet for de bedste strømforsyninger til en computer: https://www.digitaltrends.com/computing/best-pc-power-supply/ og jeg valgte nogle eksempler på strømforsyninger: "Corsair RM750" 750W, "FSP Dagger" 550W eller "Thermaltake Toughpower Grand RGB" 650W

8. Hvis vi til beregning overvejer kilden "FSP Dagger", er effektværdien 550W (det er den laveste effekt af eksemplerne). For 550W-kilden anvender vi samme beregning fra figur 12, kun vi erstatter 130 kWh med 550 kWh og vi får 11242 kWh.

9. Forskellen (økonomi) af energi mellem bærbar og computer er cirka 11.242 - 2.657,2 = 8.584,8 kWh

10. Lad os tænke på følgende 2 aspekter: fra et personligt synspunkt, hvis du køber en bærbar computer, vil du have en strømbesparelse efter 7 års brug på 8584,8 kWh! Hvis du ganger denne værdi med prisen på én kWh, hvilken pengebesparelse får du efter 7 års brug?

11. Fra et globalt synspunktforskellige kilder bruges til at opnå elektricitet, såsom vindkraft, kalorieenergi, vandkraft osv. Hvis du for en enkelt computer får en sådan energibesparelse, så beregnet, antag for 1000 computere med samme elektriske effekt, hvor mange naturressourcer er reddet? Men for 1.000.000 computere? Så i fremtiden, når du vil købe en computer, kan du også tænke på miljøbeskyttelsesaspektet.

12. Og nu til sidst en lille øvelse til dig. Hvis vi skulle vælge den mest kraftfulde kilde blandt dem, der er eksemplificeret med 750W, hvor meget energi ville der så være forbrugt på 7 år ud over den bærbare computer? Kan du lave denne udregning?

Trin 2: Genbrug af elektronik

Opret hypotetisk et scenarie, hvor du om natten går med en lommelygte. På et tidspunkt antages det, at der er behov for at udskifte batteriet i lommelygten med en ny opladet. Hvis det batteri ved et uheld bliver smidt et sted i naturen, vil batteriet ikke opløses som biologisk nedbrydelige stoffer, det vil eksistere der, hvor det blev smidt i lang tid. Derudover kan sure og giftige stoffer fra batteri lække og forurene området, hvor det blev dumpet, komme i grundvandet og forurene vand osv. Hvis vi tænker globalt, og ikke kun på dette batteri, er der tusindvis af tons elektrisk affald, der hvis det ikke genbruges, kan det forurene miljøet. Af denne grund er det nødvendigt at genanvende elektrisk affald, og der er lovgivning relateret til dette aspekt.

Hvordan kan du hjælpe?

Hvis du har elektrisk udstyr, som du skal smide ud (f.eks. en gammel og rusten computer eller afladede batterier), så smid dette affald på indsamlingscentrene til genbrug! På denne måde kan du skåne miljøet!

ELLER: hvis du ikke vil smide det gamle udstyr ud, og du vil have en lille indkomst fra dem (antag en gammel computer), og du har til hensigt at købe en ny, er der offentlige programmer (i Rumænien, for eksempel, er det skrotprogrammet for husholdningsapparater) for at stimulere til at forny udstyr med mere økonomiske og samtidig genbruges de gamle.

ELLER: der er handlende, som i bytte for det gamle udstyr giver rabat ved køb af andet nyt udstyr fra samme felt. Det er tilbud af typen TILBAGEKØB, der har samme effekt for genbrug af elektronisk udstyr og er mere energieffektive.

Og til sidst en lille øvelse til dig: har du en gammel computer, som du gerne vil ændre den (ikke nu, i fremtiden)? Hvis ja, så prøv at finde på internettet, hvilke købmænd der kan tilbyde dig TILBAGEKØB-løsninger?

Tillykke, du har nu gennemført modul 4.

Glem ikke at tjekke bilagene for yderligere ressourcer og dokumenter til støtte for selvstudium!

Modul 5: Problemløsning

"Problemløsning"-modulet er beregnet til dem, der er interesseret i at identificere og løse de mest almindelige hardware- og softwareproblemer, samt en sikker måde at vælge og købe de nødvendige værktøjer til at løse hverdagens problemer ved hjælp af digitale midler.

Bemærk venligst, at praktiske aktiviteter beskrevet i hver enhed kan indebære støtte fra en erfaren træner. Selvom oplysningerne i manualen er skrevet på en måde, der er let at forstå, kan nogle handlinger, der støder op til de præsenterede oplysninger, kræve støtte fra erfarne personer.

Modul 5	**Problemløsning**			
Varighed	**25 timer**			
Mål	At kunne løse almindelige og simple tekniske IKT-problemer. At kunne søge, finde og vælge den rigtige løsning til et bestemt IKT-problem. At kunne udvikle sig selv og være i kontakt med IKT-udvikling.			
Enheder	5.1 Løsning af tekniske problemer	5.2 Identificering af behov og teknologiske reaktioner	5.3 Kreativ brug af digitale teknologier	5.4 Identifikation af digitale kompetencegab
Træningsorganisation	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring	Ansigt til ansigt E-læring
Varighed	7 timer	7 timer	6 timer	5 timer

Bord 26 - Global struktur af Modul 5 – Problemløsning.

5.1 Løsning af tekniske problemer

Enhed 5.1	Løsning af tekniske problemer
Varighed	7 timer
Mål	For at kunne løse internethastighedsrelaterede problemer
Indhold	5.1.1 Computere og dets systemer 5.1.2 De mest almindelige tekniske problemer 5.1.3 Praktiske aktiviteter
Ressourcer	Træningsmanual Computer med internetforbindelse Modem
Træningsmetoder	Præsentation af træner

Bord 27- Kompetenceenhedens opbygning 5.1. – Løsning af tekniske problemer i modul 5 – Problemløsning.

5.1.1 Computere og dets systemer

"Problemløsning"-modulet er beregnet til dem, der er interesseret i at identificere og løse de mest almindelige hardware- og softwareproblemer, samt en sikker måde at vælge og købe de nødvendige værktøjer til at løse hverdagens problemer ved hjælp af digitale midler.

Hvad er en computer?

En computer er en elektronisk enhed, der manipulerer information eller data. Det har evnen til at gemme, hente og behandle data. Du ved måske allerede, at du kan bruge en computer til at skrive dokumenter, sende e-mail, spille spil og surfe på nettet. Du kan også bruge det til at redigere eller oprette regneark, præsentationer og endda videoer.

Hvad er de forskellige typer computere?

Når de fleste mennesker hører ordet computer, tænker de på en personlig computer, såsom en stationær eller bærbar computer. Computere findes dog i mange former og størrelser, og de udfører mange forskellige funktioner i vores daglige liv

Mange af nutidens elektronik er grundlæggende specialiserede computere, selvom vi ikke altid tænker på dem på den måde. Her er et par almindelige eksempler:

Tablet-computere eller tablets-er håndholdte computere, der er endnu mere bærbare end bærbare computere. I stedet for et tastatur og en mus bruger tablets en berøringsfølsom skærm til indtastning og navigation. iPad er et eksempel på en tablet.

Smartphones – Mange mobiltelefoner kan mange ting, computere kan, herunder at surfe på internettet og spille spil. De kaldes ofte smartphones, og for mange mennesker kan en smartphone faktisk erstatte elektronik som en gammel bærbar computer, digital musikafspiller og digitalkamera i den samme enhed.

Hardware vs. software

Før vi taler om forskellige typer computere, lad os tale om to ting, som alle computere har til fælles: hardware og software.

- **Hardware**er enhver del af din computer, der har en fysisk struktur, såsom tastaturet eller musen. Det inkluderer også alle computerens interne dele
- **Software**er et sæt instruktioner, der fortæller hardwaren, hvad den skal gøre, og hvordan den skal gøres. Eksempler på software omfatter webbrowsere, spil og tekstbehandlingsprogrammer

Hvad er et operativsystem (OS)?

Et operativsystem er den vigtigste software, der kører på en computer. Den administrerer computerens hukommelse og processer samt al dens software og hardware. Det giver dig også mulighed for at kommunikere med computeren uden at vide, hvordan du taler computerens sprog. Uden et styresystem er en computer ubrugelig. (Eks. operativsystemer: Windows, Linux, macO'er bruges til stationære og bærbare computere; Google Android og Apple IOS bruges til tablets og smartphones)

Hvad er en ansøgning?

Du har måske hørt folk tale om at bruge et program, en applikation eller en app, men hvad betyder det præcist? Kort sagt er en app en type software, der giver dig mulighed for at udføre specifikke opgaver. Programmer til stationære eller bærbare computere kaldes undertiden desktop-applikationer, mens applikationer til mobile enheder kaldes mobile apps.

Hvis du jævnligt bruger computere i dit daglige liv, vil du i sidste ende løbe ind i nogle tekniske problemer, som kræver din opmærksomhed. Selvom de fleste komplekse computerproblemer ofte kan løses af en specialiseret tekniker, er der mange andre små, men almindelige, problemer, der opstår regelmæssigt på en computer og hans brug i digitale miljøer. Den gode nyhed er, at mange problemer med computere har enkle løsninger, og at lære at genkende et problem og selv løse det vil spare dig for en masse tid og penge.

5.1.2 De mest almindelige tekniske problemer

1. Computeren vil ikke starte

En computer, der pludselig slukker eller har svært ved at starte op, kan have en svigtende strømforsyning. Kontroller, at computeren er tilsluttet stikkontakten korrekt, og hvis det ikke virker, test stikkontakten med en anden fungerende enhed for at bekræfte, om der er tilstrækkelig strøm.

2. Skærmen er tom

Hvis computeren er tændt, men skærmen er tom, kan der være et problem med forbindelsen mellem computeren og skærmen. Først skal du kontrollere, om skærmen er tilsluttet en stikkontakt, og at forbindelsen mellem skærmen og computerens harddisk er sikker. Hvis problemet er på en bærbar computer, skal du muligvis få en professionel til at løse det, da nogle af de interne ledninger kan være slidte.

3. Unormalt fungerende operativsystem eller software

Hvis operativsystemet eller anden software enten ikke reagerer eller virker, så prøv at genstarte din computer og kør en virusscanning. For at undgå at dette sker, skal du installere pålidelig antivirussoftware.

4. Windows vil ikke starte

Hvis du har problemer med at starte Windows, skal du muligvis geninstallere det med Windows-gendannelsesdisken.

5. Skærmen er frossen

Når din computer fryser, har du muligvis ingen anden mulighed end at genstarte og risikere at miste alt ikke-gemt arbejde. Frys kan være et tegn på utilstrækkelig ram, konflikter i registreringsdatabasen, korrupte eller

manglende filer eller spyware. Tryk og hold tænd/sluk-knappen nede, indtil computeren slukker, genstart den derefter, og gå i gang med at rense systemet, så det ikke fryser igen.

6. Computeren er langsom

Hvis din computer er langsommere end normalt, kan du ofte løse problemet ved blot at rense harddisken for uønskede filer. Du kan også installere en firewall, antivirus- og antispywareværktøjer og planlægge regelmæssige registreringsscanninger. Eksterne harddiske er gode lagringsløsninger til overbeskattede CPU'er og vil hjælpe din computer med at køre hurtigere.

7. Mærkelige lyde

Meget støj fra din computer er generelt et tegn på enten hardwarefejl eller en støjende blæser. Harddiske laver ofte støj, lige før de fejler, så det kan være en god ide at sikkerhedskopiere oplysninger for en sikkerheds skyld, og blæsere er meget nemme at udskifte.

8. Langsomt internet

For at forbedre din internetbrowsers ydeevne skal du rydde cookies og midlertidige internetfiler ofte. I Windows-søgelinjen skal du skrive '%temp%' og trykke på Enter for at åbne mappen med midlertidige filer.

9. PC overophedning

Hvis en computerkasse mangler et tilstrækkeligt kølesystem, kan computerens komponenter begynde at generere overskudsvarme under drift. For at undgå, at din computer brænder sig selv ud, skal du slukke den og lade den hvile, hvis den bliver varm. Derudover kan du tjekke blæseren for at sikre, at den fungerer korrekt.

10. Afbrudte internetforbindelser

Mislykkede internetforbindelser kan være meget frustrerende. Ofte er problemet simpelt og kan være forårsaget af et dårligt kabel eller telefonlinje, som er let at rette. Mere alvorlige problemer omfatter virus, et dårligt netværkskort eller modem eller et problem med driveren.

11. Din smartphone kører langsomt

Dette er det mest almindelige smartphone-problem, især opstår når din telefon bliver ældre. Årsagen bag den langsomme hastighed er installationen af unødvendige apps, der bruger din enheds RAM og gemmer adskillige antal filer på din telefon.

Fjern alle unødvendige apps og filer fra mobilen, ryd op i cachedata. Du kan også gøre dette ved en diagnostisk app. Hvis du stadig står over for dette problem, skal du gendanne det til fabriksdata.

12. Dårlig batterilevetid

Desværre sker dette telefonproblem for alle. De almindelige problemer er batteriafladning, langsom opladning eller opladningsfejl. Vi er klistret til vores telefon, så problemet med batteridræning er det almindelige problem. Dette store problem er, når din telefon aflades uden at blive brugt.

Find ud af, at hvis nogle bestemte apps dræner for meget batteri, kan du tjekke dette i Indstillinger->Batteri, og hvis du identificerer en fejl, skal du fjerne disse apps. Aktiver batterisparetilstand, sluk placeringerne, dæmp lysstyrken.

13. Lagerplads

Det meste af smartphone-lageret er fyldt med fotos og videoer. Du bør passe på opbevaringen, når du køber en ny smartphone, fordi du efter et par dage begynder at gå i panik over den lave lagerplads. Meget få smartphones har en udvidelig hukommelsesfunktion i dag.

Slet først cachen. Brug apps som cache-rens, som lader dig rense cache for en bestemt app. Afinstaller apps, eller flyt apps fra telefonen. Overfør billederne til skyer for at frigøre plads på din enhed.

14. Telefon eller app går ned

Dette sker, når der er en fejl i de installerede apps, eller din telefon løber tør for plads. Dette er et af de frustrerende mobiltelefonproblemer.

Ryd appdataene fra "App manager". Undgå at bruge flere apps på samme tid. Fejlfind din telefon ved at genstarte enheden, fjerne batteriet eller gendanne den til fabriksindstillingerne.

15. Smartphone overophedning

Overdreven brug af smartphone giver problemer med overophedning. Krævende apps, mere sandsynlige gaming apps gør temperaturen høj på din telefon, hvilket kan påvirke batteriets ydeevne. Måske har du downloadet ondsindede apps, der kører i baggrunden.

Prøv ikke at bruge din telefon, mens den er opladet. Brug ikke apps, der suger høj CPU, og giv en pause til din telefon. Hvis din telefon stadig varmer, er dette producentfejlen.

16. Forbindelsesproblem med Bluetooth, wifi, mobilnetværk

Dette er det midlertidige mobiltelefonproblem, som nemt kan løses. Hold telefonen i flytilstand i 30 til 60 sekunder, og prøv at tilslutte den igen. Har du stadig et problem? Reparer eller skift indstillingen af Bluetooth og WiFi igen.

17. Apps downloades ikke

Hovedårsagen til dette problem er korrupt cache. Gå til appen Google Play Butik, og ryd cachen i appen. Bedre at slette historien om Google Play Butik. Sørg for, at du bruger den nyeste version af Google Play Butik. Hvis der stadig er et problem, skal du rydde data og cache på Google Play-tjenester.

18. Synkroniseringsproblem

Synkroniseringsproblemet bliver løst automatisk efter nogen tid. Hvis ikke, skal du fjerne Google-kontoen og tilføje den igen. Sørg for, at din internetforbindelse ikke er begrænset og fungerer korrekt. Se efter systemopdateringen, og opdater den, hvis det er nødvendigt.

19. MicroSD-kort virker ikke på din smartphone

Det kan være forårsaget, når dit SD-kort har dårlige læse-/skrivefejl. Din mobil genkender ikke SD-kortet efter formatering. Tjek hukommelseskortets kapacitet, og formater det til exFAT, hvis det er op til 32 GB. Genstart telefonen i gendannelsestilstand, og vælg tør cache i Android. Dette vil rydde SD-kortet ud og formatere det til FAT32, som er bedst egnet til lagring i en telefon.

20. Revnet skærm eller nedsænkning i vand

Dette mobiltelefonproblem opstår ved et uheld, og vi kan ikke gøre noget ved dette. For at undgå sådanne hændelser skal du bruge den gode telefonbeskytter. Ja, de kan være dyre, men det er en værdig investering for at undgå disse ulykker.

En computer er en elektronisk enhed, der manipulerer information eller data. Det har evnen til at gemme, hente og behandle data. Du ved måske allerede, at du kan bruge en computer til at skrive dokumenter, sende e-mail, spille spil og surfe på nettet. Du kan også bruge det til at redigere eller oprette regneark, præsentationer og endda videoer.

5.1.2 Praktiske aktiviteter

Trin 1: Genstart dit modem og dine trådløse enheder

Når du har tilsluttet dit modem og opsat dit hjemmenetværk, bør både dine kablede og trådløse internetforbindelser være pålidelige hver dag. Langsomme hastigheder og afbrydelser kan skyldes svage signaler, gammelt udstyr eller kabler, interferens, enhedskapacitet/begrænsninger og muligvis tredjepartsrelaterede problemer. Hvis du tror, der er et problem med dit WiFi, så prøv de nemme løsninger, der er skitseret nedenfor for at løse de mest almindelige problemer.

En simpel genstart af dit modem kan løse mange WiFi- eller forbindelsesproblemer

1. Tag strømkablet ud af bagsiden af WiFi-modemet eller fra stikkontakten.
2. Vent 30 sekunder.
3. Tilslut strømkablet til modemmet igen.

Inden for et par minutter skulle dit WiFi-netværk dukke op igen på listen over tilgængelige netværk på dine trådløse enheder. Prøv at tilslutte en enhed til WiFi for at se, om det virker.

Genstart af dine trådløse enheder kan også være løsningen på mange almindelige problemer, herunder forsinkelser eller tab af internetadgang. Se din enhedsmanual om, hvordan du udfører en standardgenstart.

Trin 2: Modemplacering og dækning

Placeringen af dit modem i dit hjem spiller en væsentlig rolle for din WiFi-dækning og er en nøglefaktor for en stabil WiFi-forbindelse. For bedre WiFi-dækning bør dit modem placeres centralt, dette fungerer især godt, hvis du har et åbent planløsningshus. Alternativt er det et godt valg at placere dit modem centralt i forhold til det sted, hvor internettet oftest bruges. Sørg for, at du placerer dit modem

✓ Ude i det fri

✓ Rejst fra jorden

Undgå at placere dit modem

✕ I kældre

✕ I skabe

✕ Bag andre genstande

For at undgå interferens skal du prøve at holde dit modem væk fra

✕ Husholdningsapparater

✕ Metalgenstande

✕ Elektrisk udstyr

Trin 3: Tjek dine forbindelser

Løse forbindelser, beskadigede kabler og linjesplittere kan forringe internetsignaler, før de overhovedet når dit modem og forhindre dig i at nå højere internethastigheder. For at løse dette skal du sikre dig, at dine kabler er korrekt tilsluttet.

1. Tag strømkablet ud af modemmets bagside.
2. Skru koaksialkablet af bagsiden af modemmet.
3. Undersøg koaksialkablet for bøjninger eller knæk, der indikerer beskadigelse.
4. Følg koaksialkablet til kabelstikket på væggen.
5. Bestem, om koaksialkablet går direkte ind i stikket, eller om det passerer gennem andre enheder, såsom en splitter.
6. Hvis der er en splitter til stede, skal du midlertidigt fjerne splitteren, så koaksiallinjen kan forbinde kabelstikket direkte til modemmet.
7. Tilslut koaksial- og strømkablerne til bagsiden af dit modem igen.
8. Vent på, at modemmet kommer online igen.

Hvis du bruger et Ethernet-kabel til at forbinde din computer til routeren eller dit modem til en tredjepartsrouter, skal du også inspicere disse kabler og udskifte dem, hvis de ser beskadigede ud.

Trin 4: Gendan modemindstillinger

I nogle sjældne tilfælde kan det hjælpe at gendanne dit modem til dets fabriksindstillinger som en sidste udvej, hvilket vil nulstille alle brugerdefinerede indstillinger, du måtte have opsat, inklusive dit Wi-Fi-netværksnavn og adgangskode til deres standardindstillinger, som findes på klistermærket på dit modem.

Sådan gendannes dit modem:

1. Find den lille nulstillingsknap på dit modem.
2. Tryk og hold knappen nede med en papirclips eller nål i 15 sekunder.
3. Se modemets lys blinke, og forblive tændt efter et par øjeblikke.

Inden for et par minutter skulle dit Wi-Fi-netværk dukke op igen på listen over tilgængelige netværk på dine trådløse enheder. Prøv at tilslutte en enhed til Wi-Fi for at se, om det virker.

5.2 Identificering af behov og teknologiske reaktioner

Enhed 5.2	Identificering af behov og teknologiske reaktioner
Varighed	7 timer
Mål	At kunne løse almindelige og simple tekniske IKT-problemer.
Indhold	5.2.1 Identifikation af behov og teknologiske reaktioner 5.2.2 Praktiske aktiviteter
Ressourcer	Træningsmanual Computere med internetadgang
Træningsmetoder	Præsentation af træner

Bord 28- Kompetenceenhedens opbygning 5.2. – Identificering af behov og teknologiske reaktioner i modul 5 – Problemløsning.

5.2.1 Identificering af behov og teknologiske reaktioner

Det første skridt, når det kommer til at løse ethvert computerproblem, er at finde ud af, hvilken komponent der ikke fungerer korrekt. Nogle gange skyldes det noget simpelt, såsom at lyden ikke virker, eller vi kan ikke rigtigt se, at skærmen eller tastaturet/musen er holdt op med at virke. Andre gange starter computeren ikke engang, den genstarter eller slukker pludselig, og vi ved ikke, hvad der sker. For at identificere problemet skal vi være opmærksomme på de spor, som computeren giver os.

Der er mange forskellige ting, der kan forårsage et problem med din computer. Uanset hvad der forårsager problemet, vil fejlfinding altid være en proces med forsøg og fejl, i nogle tilfælde skal du muligvis bruge flere

forskellige tilgange, før du kan finde en løsning; andre problemer kan være nemme at løse. Vi anbefaler at starte med at bruge følgende tips.

- **Skriv dine trin ned**: Når du begynder at fejlfinde, vil du måske skrive ned hvert trin, du tager. På denne måde vil du være i stand til at huske præcis, hvad du har gjort, og kan undgå at gentage de samme fejl. Hvis du ender med at bede andre mennesker om hjælp, vil det være meget nemmere, hvis de ved præcis, hvad du allerede har prøvet.
- **Tag noter om fejlmeddelelser**: Hvis din computer giver dig en fejlmeddelelse, skal du sørge for at skrive så mange oplysninger ned som muligt. Du kan muligvis bruge disse oplysninger senere til at finde ud af, om andre mennesker har den samme fejl.
- **Kontroller altid kablerne**: Hvis du har problemer med et bestemt stykke computerhardware, såsom din skærm eller tastatur, er et nemt første trin at tjekke alle relaterede kabler for at sikre, at de er korrekt tilsluttet.

- **Genstart computeren**: Når alt andet fejler, er det en god ting at prøve at genstarte computeren. Dette kan løse en masse grundlæggende problemer, du kan opleve med din computer.

- **Brug af elimineringsprocessen**: Hvis du har et problem med din computer, kan du muligvis finde ud af, hvad der er galt ved hjælp af elimineringsprocessen. Det betyder, at du laver en liste over ting, der kan være årsag til problemet, og derefter teste dem én efter én for at fjerne dem. Når du har identificeret kilden til dit computerproblem, vil det være lettere at finde en løsning.

Søg på internettet

Du kan finde nogle løsninger gennem tusindvis af videoøvelser på YouTube eller fra onlinekilder, der giver trinvise instruktioner om computerfejlfinding.

Hvad er en video tutorial?

Det er en videoguide til, hvordan man løser et specifikt problem.

Hvad er formålet med video tutorial?

Videotutorials tilbyder en multidimensionel oplevelse, der kan kombinere diagrammer, dias, fotos, grafik, fortælling, skærmbilleder, billedtekster på skærmen, musik og live video. Dette giver elever med forskellige indlæringsevner mulighed for at opbevare information i en metode, der er mere egnet til dem.

For eksempel, hvis du ønsker at installere en printer, kan du skrive på en søgemaskine "printer installation tutorial". Et af resultaterne er en video med navnet: Konfigurer eller installer en printer på Windows 10|How-Tohttps://www.youtube.com/watch?v=E83yneh4xCA, klik på den og følg trin-for-trin oplysningerne om printerinstallation.

Online kilder: Websteder, der kan give dig den rette knowhow inden for computerfejlfinding og teknisk support.

Eksempel: Blødende computer: http://www.bleepingcomputer.com

Siden er en fremragende kilde til information, råd og tutorials om computersoftware og hardware, fejlfinding og sikkerhed, for at nævne nogle få. Det har en søgbar database med artikler, der opdateres månedligt af dens stabile af regelmæssige bidragydere.

Eksempler på hardwarebehov:

- **web kamera**: Et webcam er et videokamera, der feeder eller streamer et billede eller en video i realtid til eller gennem et computernetværk, såsom internettet. Webcams er typisk små kameraer, der sidder på et skrivebord, fastgøres til en brugers skærm eller er indbygget i hardwaren.
- **Printer**: en maskine til udskrivning af tekst eller billeder, især en der er knyttet til en computer.
- **Scanner**: en enhed, der scanner dokumenter og konverterer dem til digitale data.
- **Mikrofon**: En mikrofon (forkortet mikrofon) er en elektronisk enhed, der konverterer lydbølger til elektroniske signaler, som derefter tages af computeren som input. På stationære computere er det meget som enhver anden perifer enhed og er normalt tilsluttet separat.
- **Lydhøjttalere**: Højttalere er transducere, der omdanner elektromagnetiske bølger til lydbølger. Højttalerne modtager lydinput fra en enhed, såsom en computer eller en lydmodtager. ... Lyden produceret af højttalere er defineret af frekvens og amplitude. Frekvensen bestemmer, hvor høj eller lav lydens tonehøjde er.
- **Smartphone kamera**: Smartphones, der er kameratelefoner, kan køre mobilapplikationer for at tilføje funktioner såsom geotagging og billedsammensætning. ... Fra midten af 2010'erne har nogle avancerede kameratelefoner optisk billedstabilisering (OIS), større sensorer, lysstærke objektiver, 4K-video og endda optisk zoom.
- **Porte og forbindelser**: I computerhardware fungerer en port som en grænseflade mellem computeren og andre computere eller perifere enheder. I computertermer refererer en port generelt til den del af en computerenhed, der er tilgængelig for tilslutning til eksterne enheder, såsom input- og outputenheder.
- **Trådløs teknologi**: Trådløs teknologi giver mulighed for at kommunikere mellem to eller flere enheder over afstande uden brug af ledninger eller kabler af nogen art. Nogle af disse termer kan være bekendte for dig: radio- og tv-udsendelser, radarkommunikation, mobilkommunikation, globale positionssystemer (GPS), Wi-Fi, Bluetooth og radiofrekvensidentifikation er alle eksempler på "trådløs" med meget forskellige anvendelser i nogle tilfælde.

Eksempler på softwarebehov:

- **Filudvidelser**: Filudvidelser er en måde at mærke navnene på filer på, så du og din computer kan holde styr på, hvad de indeholder. ... Den sidste del af filnavnet bruges til at angive filtypen, så computeren kan åbne det korrekte program, når du vil bruge filen.
  Windows bruger filtypenavne til at bestemme, hvordan det åbner forskellige typer filer. Når en bruger dobbeltklikker på en fil for at åbne den, åbner Windows den med det program, der er knyttet til filens filtypenavn. Windows-systemkonfigurationen vedligeholder en liste over programmer og deres tilknyttede filtypenavne. Disse kaldes "standardprogrammer". Hvis en bestemt filtypenavn er

registreret med et program, vil Windows starte dette program, hver gang brugeren vælger at åbne en fil med denne filtype. Der kan dog kun registreres ét program som standardprogram for hver filtypenavn. For at bruge et andet program end standardprogrammet til at åbne en fil, skal du højreklikke på filen og vælge "Åbn med".

- **Opdater software**: Softwareopdateringer er vigtige, fordi de ofte indeholder kritiske patches til sikkerhedshuller. ... De kan også forbedre stabiliteten af din software og fjerne forældede funktioner. Alle disse opdateringer har til formål at gøre brugeroplevelsen bedre
- **Antivirus installation:** Antivirussoftware hjælper med at beskytte din computer mod malware og cyberkriminelle. Antivirussoftware ser på data – websider, filer, software, applikationer – der rejser over netværket til dine enheder. ... Det søger at blokere eller fjerne malware så hurtigt som muligt.
- **Skærmindstillinger**: Din computer har en række skærmindstillinger, der giver dig mulighed for at tilpasse din seeroplevelse baseret på din aktivitet. Dine skærmindstillinger kan justeres alt efter, hvad du bruger din computer til, og hvilken type skærm du har

5.2.2 Praktiske aktiviteter

Trin 1: Genstart din telefon

1. På de fleste telefoner skal du trykke på telefonens tænd/sluk-knap i cirka 30 sekunder, eller indtil din telefon genstarter
2. På skærmen skal du muligvis trykke på Genstart.

Trin 2: Se efter Android-opdateringer

Vigtigt: Indstillinger kan variere fra telefon til telefon.

1. Åbn din telefons Indstillinger-app.
2. Tryk på System tæt på bunden › Fremskreden › Systemopdatering. Hvis det er nødvendigt, skal du først trykke på Om telefon eller Om tablet.
3. Din opdateringsstatus vises. Følg alle trin på skærmen.

Trin 3: Tjek lagerplads og frigør plads

Din telefon kan begynde at få problemer, når mindre end 10 % af lagerpladsen er gratis. Hvis du mangler lagerplads,nedenfor kan du finde information om, hvordan du frigør plads.

Slet billeder og videoer

1. Åbn Google Fotos-appen på din Android-telefon eller -tablet.
2. Log ind på din Google-konto.

3. Tryk og hold på et billede eller en video, du vil flytte til papirkurven. Du kan vælge flere elementer.
4. Tryk på Papirkurv øverst.

På de fleste telefoner kan du tjekke, hvor meget lagerplads du har til rådighed i appen Indstillinger. Indstillinger kan variere fra telefon til telefon.

Tøm dit skraldespand

Hvis du ser en anmodning om "Slet permanent", når du forsøger at flytte et element til papirkurven, er din papirkurv fuld. Din skraldespand kan rumme 1,5 GB.

Vigtigt: Hvis du tømmer din papirkurv, sletter du permanent alle elementer i din papirkurv.

1. Åbn Google Fotos-appen på din Android-telefon eller -tablet.
2. Log ind på din Google-konto.
3. Tryk på Bibliotek nederst > Affald > Mere > Tømme skrald > Slet.

Fjern downloadede film, musik og andre medier

Sådan sletter du indhold fra Google Play:

1. Åbn Google Play-appen med indholdet, f.eks. Play Musik eller Play Film og TV.
2. Tryk på menuen > Indstillinger > Administrer downloads.
3. Tryk på Downloadet > Fjerne.

For at slette indhold fra andre kilder skal du slette fra den app, du brugte til at downloade det.

Trin 4: Luk apps, der ikke reagerer

Android administrerer den hukommelse, som apps bruger. Du behøver normalt ikke at lukke apps, men hvis en app ikke reagerer, kan du prøve at lukke appen.

Trin 5: Opdater app

1. Åbn appen Google Play Butik på din telefon.

2. Tryk på Menu ☰ > Mine apps og spil.
3. Apps med tilgængelige opdateringer er mærket "Opdater".
    - Hvis en opdatering er tilgængelig, skal du trykke på Opdater.
    - Hvis flere opdateringer er tilgængelige, skal du trykke på Opdater alle.

Trin 6: Afinstaller apps, du ikke bruger

Forsigtig: Alle data gemt i denne app vil blive slettet.

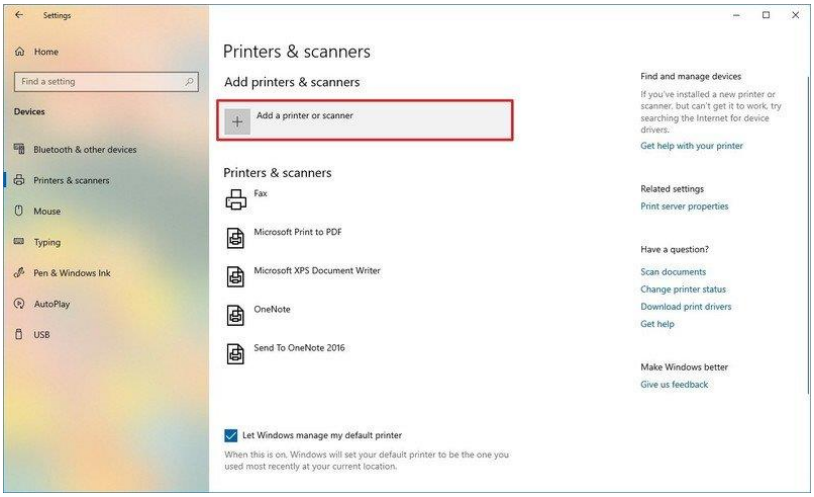
1. Tryk og hold på den app, du vil afinstallere.
2. For at se dine muligheder skal du begynde at trække i appen.
3. Træk appen til Afinstaller øverst på skærmen. Hvis du ikke kan se "Afinstaller", kan du ikke afinstallere appen.
4. Løft fingeren.

Tip: Hvis du vil bruge appen igen, kan du prøve at geninstallere den.

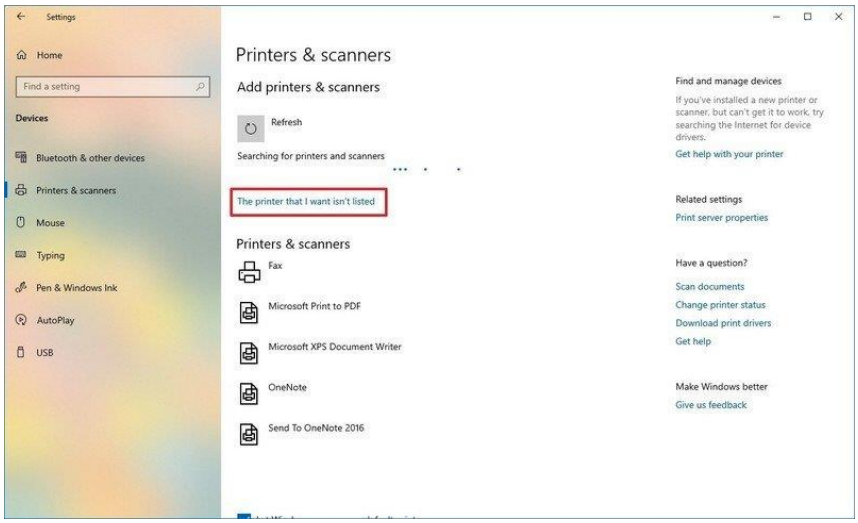
Installation af en lokal printer manuelt

Når systemet ikke registrerer din printer automatisk, kan du stadig tilføje enheden manuelt afhængigt af forbindelsestypen og printerens alder.
Vigtig:Før du fortsætter, skal du sørge for, at din computer er forbundet til internettet for at tillade Windows Update at downloade yderligere drivere.

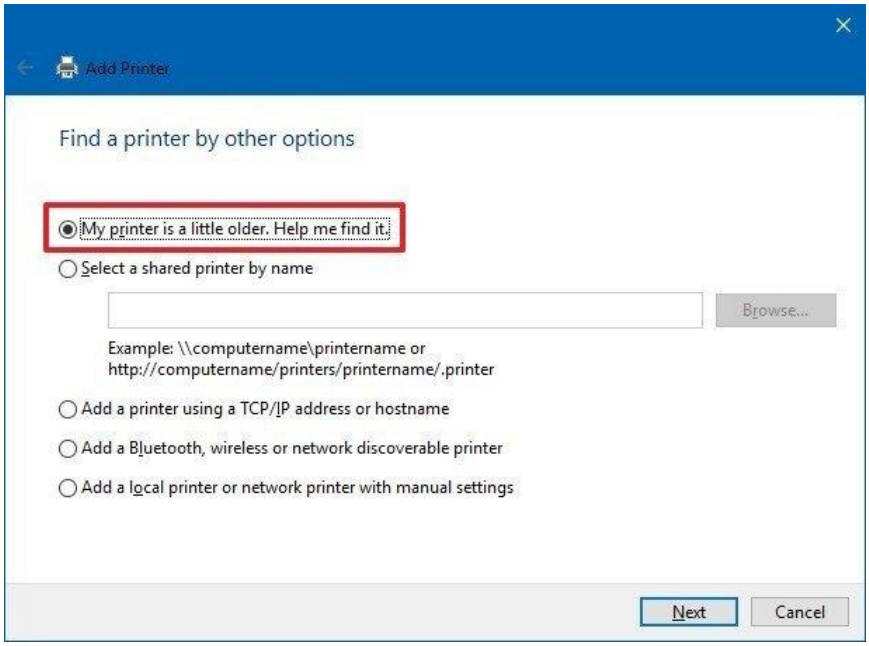
1. Åbn Indstillinger.
2. Klik på Enheder.
3. Klik på Printere og scannere.
4. Klik på knappen Tilføj en printer eller scanner.



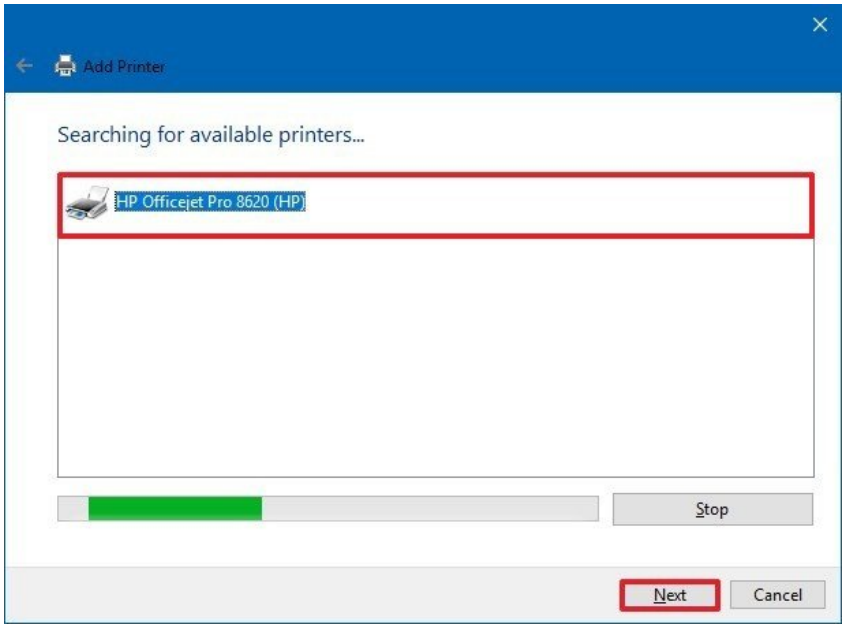
5. Vent et øjeblik.
6. Klik på Den printer, jeg ønsker, er ikke på listen.



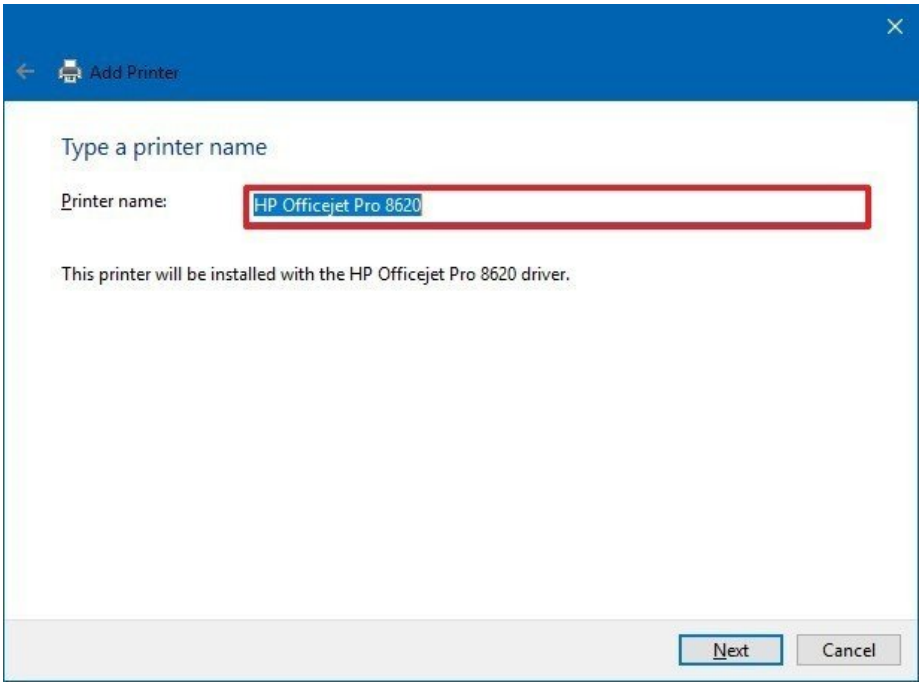
7. Vælg Min printer er lidt ældre. Hjælp mig med at finde den mulighed.



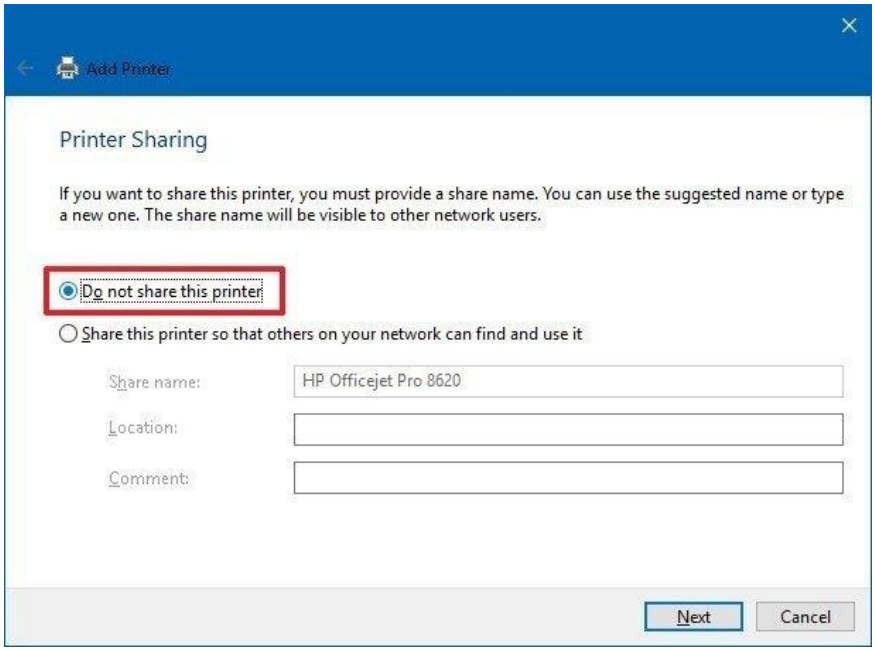
8. Vælg din printer fra listen.
9. Klik på knappen Næste.



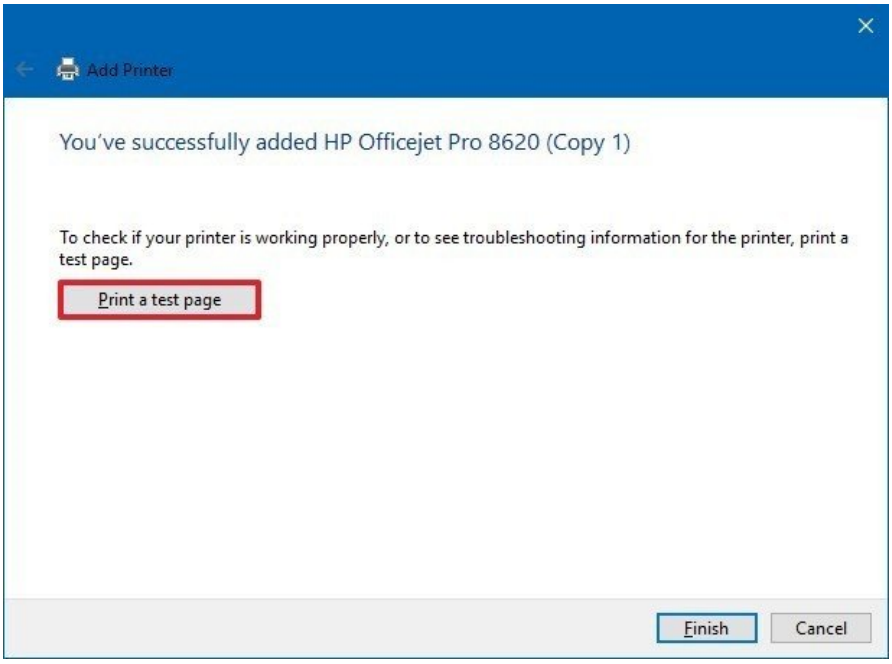
10. Indtast et navn til printeren.
11. Klik på knappen Næste.



12. Vælg indstillingen Del ikke denne printer.
13. Klik på knappen Næste.



14. Klik på indstillingen Udskriv en testside for at bekræfte, at enheden fungerer.



15. Klik på knappen Udfør.

Når du har gennemført trinene, bør du være i stand til at begynde at udskrive til enheden.

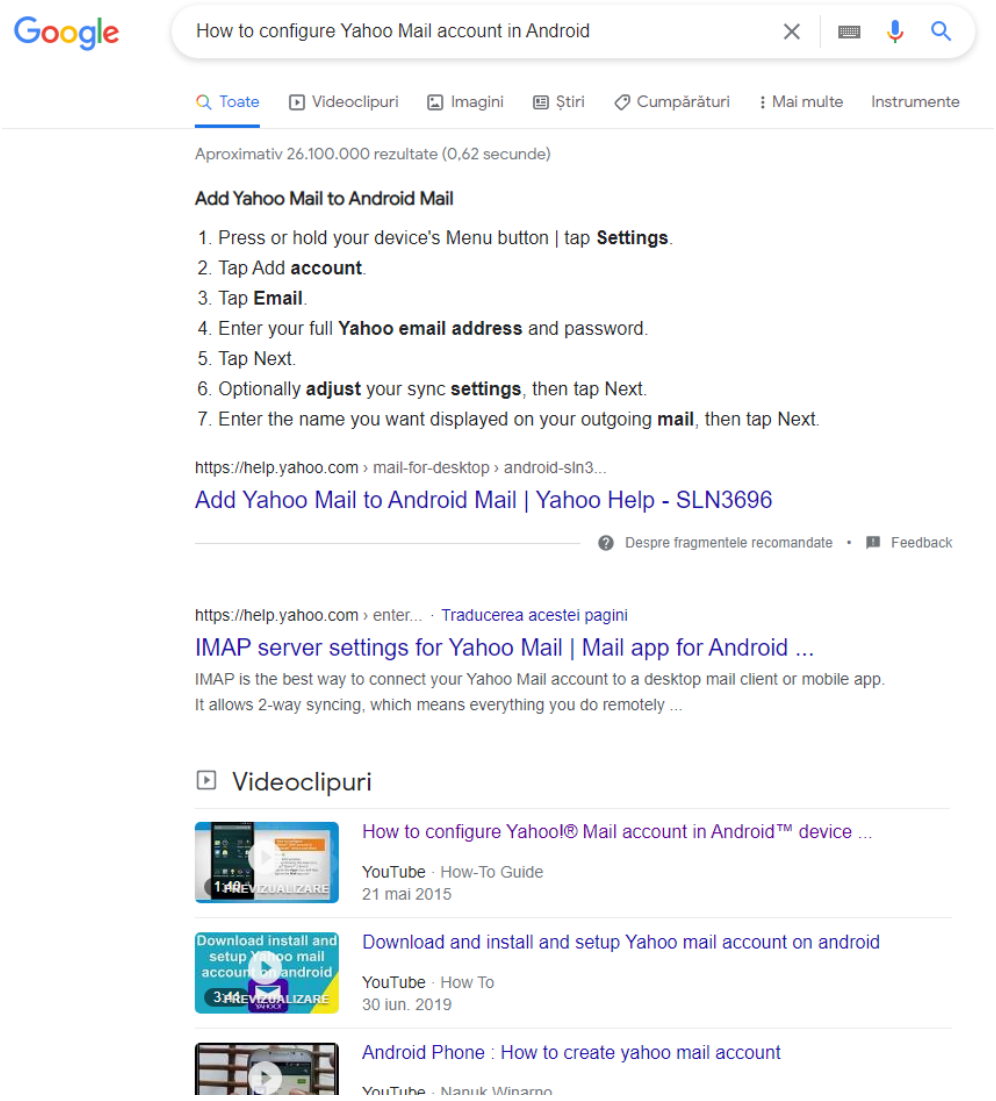
Sådan konfigureres Yahoo!® Mail-konto i Android™-enhedens mailklient

Vil du tjekke din Yahoo!® Mail-kontos e-mails på din Android™-enhed? Hvis du vil konfigurere Yahoo!® Mail-konto i din smartphone-enheds mailklient, kan du bruge en videovejledning til at hjælpe dig med at løse denne situation.

1. Åbn en browserside, og skriv navnet på en søgemaskine F.eks. Google.

2. Skriv "Sådan konfigurerer du Yahoo Mail-konto i Android" på linjen i Google-søgemaskinen.

3. Mange resultater vises på skærmen. Vælg et af videoresultaterne for søgekriterierne, og dobbeltklik på det. Eks. Første video :(https://www.youtube.com/watch?v=C0KxJ-T7rRw)



4. Se denne video, og følg trinene for at gøre det.

Bed publikum om at give eksempler på behov og gentag søgningen efter selvstudier i overensstemmelse med deres svar.

5.3 Kreativ brug af digitale teknologier

Enhed 5.3	Kreativ brug af digitale teknologier
Varighed	6 timer
Mål	Forstå og udforske kreative digitale teknologier
Indhold	5.3.1 Digital kreativitet 5.3.2 Praktiske aktiviteter
Ressourcer	Træningsmanual Computere med internetadgang
Træningsmetoder	Præsentation af træner Gruppeøvelse Diskussion / Debat Arbejde i par/små grupper

Bord 29- Kompetenceenhedens opbygning 5.3. – Kreativ brug af digitale teknologier fra Modul 5 – Problemløsning.

5.3.1 Digital kreativitet

Kreativitet er hurtigt ved at blive en af de mest værdsatte egenskaber i det 21. århundrede, og ifølge en rapport fra 2016 fra World Economic Forum er det en af de tre bedste færdigheder, som arbejdsgivere vil være på udkig efter i 2020. En undersøgelse fra IBM fandt også at 60 % af administrerende direktører mener, at kreativitet er den vigtigste lederskabskvalitet i dag.

Digital kreativitet er et nyt, dynamisk, tværfagligt og hastigt voksende felt. Mens der er en voksende klarhed over, hvad kreativitet er meningen med digital, udvides dagligt. Ikke overraskende kan digital kreativitet betyde mange ting for forskellige i erhvervslivet, den tredje sektor, i uddannelse og i uformel læring.

Ny hardware/software giver utvivlsomt unge mennesker mulighed for at engagere sig i verden, ofte legende og eksperimenterende, på måder, som de ikke kunne have gjort selv for ti år siden. Digital kreativitet er bestemt forbløffende hurtig og er efter al sandsynlighed mere end summen af digital + kreativitet.

Eksempler på digital kreativitet:

- **Tekstbehandling**. Inden for databehandling refererer udtrykket tekstbehandling til teorien og praksisen om at automatisere oprettelsen eller manipulationen af elektronisk tekst. ... Begrebet behandling refererer til automatiseret (eller mekaniseret) behandling, i modsætning til den samme manipulation udført manuelt.
- **Medie redigering**. Redigering er processen med at udvælge og forberede skriftligt, fotografisk, visuelt, hørbart eller filmisk materiale, der bruges af en person eller en enhed til at formidle et budskab eller information.
- **Design af præsentationer**. Hvad er præsentationsdesign? Præsentationsdesignere laver en række ideer, historier, ord og billeder til et sæt dias, der er arrangeret for at fortælle en historie og overtale et publikum.
- **E-mail**. E-mail er et system til at sende skriftlige beskeder elektronisk fra en computer til en anden. E-mail er en forkortelse af 'elektronisk post'.
- **Sociale medier**. Sociale medier er en computerbaseret teknologi, der letter deling af ideer, tanker og information gennem opbygning af virtuelle netværk og fællesskaber. De sociale medier er designmæssigt internetbaserede og giver brugerne hurtig elektronisk kommunikation af indhold.
- **Datavisualisering**. Datavisualiseringer den grafiske repræsentation af information og data. Ved at bruge visuelle elementer som diagrammer, grafer og kort giver datavisualiseringsværktøjer en tilgængelig måde at se og forstå tendenser, outliers og mønstre i data.

Digitale kreativitetsværktøjer

- **Kalendere:** En digital kalender lader dig gå så langt ud, som du har brug for, se de tilbagevendende begivenheder, du vil have, og planlægge noget til 2031, som om det var næste uge. Du har den altid med dig. Sandsynligvis. Hvor vidunderlig en papirplanlægger end er, så er den endnu en ting at have med sig.

- **Foto redigering app**: Et billedredigeringsprogram til digitale fotos. Det bruges til at beskære og retouchere billeder samt organisere dem i album og diasshow. Fotoredigeringsværktøjer har typisk ikke de utallige filtre og funktioner, som en fuld-blæst billededitor som Adobes Photoshop eller Corel's Paint Shop Pro.

- **App til tekstredigering**: En teksteditor er en type computerprogram, der redigerer almindelig tekst. Teksteditorer leveres med operativsystemer og softwareudviklingspakker og kan bruges til at ændre filer såsom konfigurationsfiler, dokumentationsfiler og programmeringssprogskildekode.

- **Sociale medier app**: Sociale medier apps er applikationer, som enten kan downloades og gemmes på din telefon eller tablet eller streames gennem din internetbrowser. Sociale medier apps involverer generelt beskeder, fotodeling og interaktivt indhold. Facebook, Instagram, Twitter.

5.3.2 Praktiske aktiviteter

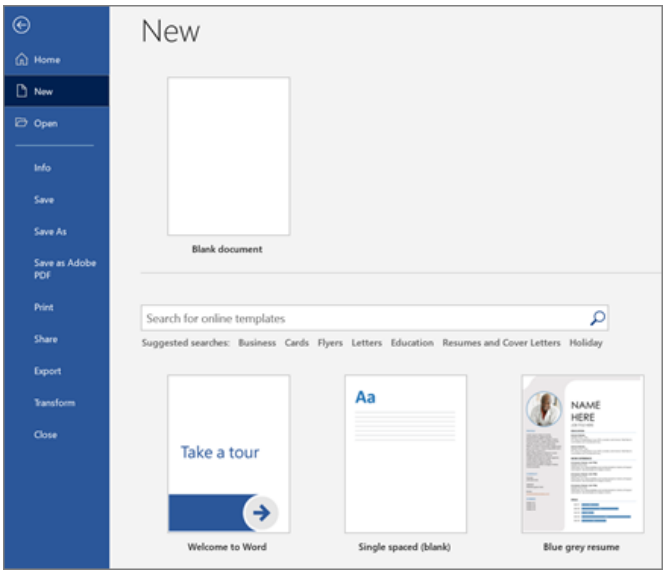
Trin 1: Opret et dokument

1. Åbn en tekstapp f.eks. Fru Word.

2. Klik på Ny på fanen Filer.

3. Indtast den type dokument, du vil oprette, i feltet Søg efter online skabeloner, og tryk på ENTER.

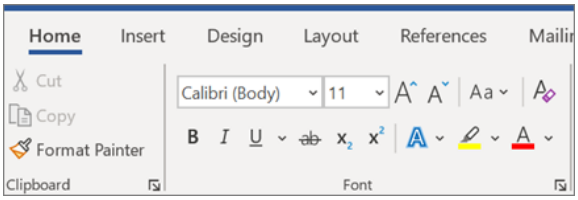
Tip: For at starte fra bunden skal du vælge Tomt dokument eller for at øve dig i at bruge Word-funktioner, prøv en læringsvejledning som Velkommen til Word, Indsæt din første indholdsfortegnelse og mere.



4. Tilføj og formater tekst

    1. Placer markøren og skriv noget tekst.

2. For at formatere skal du vælge teksten og derefter vælge en indstilling: Fed, Kursiv, Punkttegn, Nummerering og mere.



5. Tilføj billeder, figurer, SmartArt, diagram og mere

1. Vælg fanen Indsæt.
2. Vælg, hvad du vil tilføje:
    - Tabeller - vælg Tabeller, hold musemarkøren over den ønskede størrelse, og vælg den.
    - Billeder - vælg Billeder, søg efter det ønskede billede, og vælg Indsæt.
    - Online billeder - vælg Online billeder, søg og vælg det billede, du ønsker, og vælg Indsæt.
    - Figurer - vælg Figurer, og vælg derefter en figur fra rullemenuen.
    - Ikoner - vælg Ikoner, vælg den du ønsker, og vælg Indsæt.
    - 3D-modeller - vælg 3D-modeller, vælg fra en fil eller onlinekilde, gå til det billede, du ønsker, og vælg Indsæt.
    - SmartArt - vælg SmartArt, vælg en SmartArt-grafik, og vælg OK.
    - Kort - vælg Kort, vælg det ønskede diagram, og vælg OK.
    - Skærmbillede - vælg Skærmbillede, og vælg et fra rullemenuen.

6. Udskriv et dokument i Word

1. Klik på Filer > Udskriv.
2. For at få vist hver side, skal du klikke på frem- og tilbagepilene nederst på siden. Hvis teksten er for lille til at blive læst, skal du bruge zoomskyderen nederst på siden for at forstørre den.
3. Vælg antallet af kopier og eventuelle andre muligheder, og klik på knappen Udskriv.

Trin 2: Opret et opslag på sociale medier

Følg de næste trin for at oprette et opslag på Facebook, både i mobilappen og på Facebooks hjemmeside. Indlæg kan indeholde tekst, billeder, videoer og placeringsdata. Du kan skrive på din egen side, en vens side eller på siden i en gruppe, som du er en del af.

1. Åbn Facebook. Facebook-appikonet ligner et hvidt "f" på en mørkeblå baggrund. Facebook åbner for dit nyhedsfeed, hvis du allerede er logget ind.

Hvis du ikke allerede er logget ind, skal du indtaste din e-mailadresse (eller telefonnummer) og adgangskode, og derefter trykke på Log ind.

2. Gå til den side, hvor du vil poste. Afhængigt af hvor du vil oprette dit indlæg, vil dette variere:

- Din side - Du kan oprette et indlæg til din side fra toppen af nyhedsfeedet.
- En vens side - Tryk på søgelinjen øverst på skærmen, skriv en vens navn, tryk på vedkommendes navn, og tryk derefter på vedkommendes profilbillede.
- En gruppe - Tryk på☰, tryk på Grupper, tryk på fanen Grupper, og tryk på din gruppe.

3. Tryk på postkassen.Denne boks er øverst i nyhedsfeedet. Hvis du poster på en vens side, er det under billedsektionen, der er nær toppen af deres side. Hvis du poster til en gruppe, finder du boksen lige under forsidebilledet.

- Der vil generelt være en sætning som "Skriv noget" eller "Hvad tænker du på?" i kassen.

4. Upload et billede eller en video.Tryk på Foto/Video nær midten af postskærmen, vælg derefter et billede eller en video, der skal uploades, og tryk på Udført. Hvis du gør det, føjes billedet eller videoen til dit opslag.

- Du kan trykke på flere billeder eller videoer for at uploade dem alle på én gang.
- Spring dette trin over, hvis du vil uploade et opslag, der kun er tekst.

5. Tilføj tekst til dit indlæg.Tryk på tekstfeltet, og skriv derefter teksten til dit indlæg.

- Du kan også trykke på en farvet cirkel langs midten af skærmen for at angive en baggrund for dit indlæg. Du kan kun tilføje farve til indlæg med 130 tegn eller derunder.

6. Tryk på Føj til dit indlæg. Det er midt på skærmen. Dette vil vise følgende indlægsmuligheder:

- Foto/video - Tilføj flere billeder eller videoer.

- Tjek ind - Giver dig mulighed for at tilføje en adresse eller lokation til dit indlæg.
- Følelse/Aktivitet/Klistermærke - Lader dig tilføje en følelse, aktivitet eller emoji.
- Tag personer - Giver dig mulighed for at tilføje en person til dette indlæg. Gør du det, placeres indlægget også på deres side.

7. Vælg en postindstilling for at tilføje flere til indlægget.Dette er helt valgfrit. Hvis du ikke ønsker at tilføje flere til indlægget, skal du springe til næste trin.

8. Tryk på Send. Det er i øverste højre hjørne af skærmen. Hvis du gør det, oprettes dit opslag og føjes det til den side, du er på.

5.4 Identificering af digitale kompetencegab

Enhed 5.4	Identificering af digitale kompetencegab
Varighed	5 timer
Mål	At kunne bruge teknologier til at interagere med andre
Indhold	5.4.1 Den digitale kvalifikationskløft i Europa 5.4.2 Praktiske aktiviteter
Ressourcer	Træningsmanual Computer med internetadgang
Træningsmetoder	Præsentation af træner Arbejde i par/små grupper

Bord 30- Kompetenceenhedens opbygning 5.4. – Identifikation af mangler i digitale kompetencer i Modul 5 – Problemløsning

5.4.1 Den digitale kvalifikationskløft i Europa

Digitale teknologier bruges i mange sektorer såsom landbrug, sundhedspleje, transport, uddannelse, detailhandel, automatik, energi, skibsfart, logistik, undervisning og informations- og kommunikationsteknologiindustrien. Efterspørgslen efter informations- og kommunikationsteknologispecialister vokser hurtigt. I fremtiden vil 9 ud af 10 job kræve digitale færdigheder. Samtidig har 169 millioner europæere mellem 16 og 74 år – 44 % – ikke grundlæggende digitale færdigheder

Som noget andet, hvis du vil vokse inden for dette felt, skal du fortsætte med at lære.

Eleverne vil være i stand til at finde ud af, hvilke forbedringer de skal foretage for at tilegne sig eller forbedre de færdigheder og kompetencer, der er nødvendige for at klare sig så godt som muligt i deres (fremtidige) rolle. I sidste ende vil dette også have en positiv indflydelse på din dagligdag.

1. **Invester i uddannelse.** Websteder som Udemy og Skillshare har nogle geniale kurser om en lang række digitale emner. FraSEOog Google Analytics til Social Media og Content Marketing, vil du være sikker på at finde noget i det område, du leder efter at lære mere om. Sørg altid for at tjekke anmeldelserne, før

du køber et kursus, og se, hvor lang tid det vil tage at gennemføre. Nogle kurser kan gennemføres på en dag, mens andre vil kræve mere tid.

2. **Tryk på abonner.** Når du støder på en virkelig nyttig artikel, skal du trykke på abonner på hjemmesiden for at modtage fremtidige nyhedsbreve. Det er det værd, når indholdet virkelig skiller sig ud for dig, da fremtidige artikler sandsynligvis vil være lige så nyttige.

   Sørg dog for at gøre dette selektivt, da det sidste du ønsker er at blive bombarderet. Ved at filtrere det overlegne indhold fra, vil du vide, hvornår en e-mail lander i din indbakke, det er værd at læse.

3. **Deltag i grupper**. Fællesskaber, fora og onlinegrupper kan være en god ressource til at holde sig opdateret på dette område. Lær af andre og del dine erfaringer i løbende samtaler. Bare sørg for at fortsætte med forsigtighed, da nogle grupper kan indeholde en masse spam og irrelevant information.

   Søg på Facebook og LinkedIn efter grupper i din niche, uanset om det er digital markedsføring generelt eller noget mere specifikt såsom e-handel eller sociale medier. Husk, jo mere specifik du er, jo mere relevante vil samtalerne og indlæggene være.

4. **Kom ombord med Google Alerts**. Dette smarte værktøj er en fantastisk måde at holde sig ajour med trends og tips. Du skal blot fortælle Google, hvilke søgeord du gerne vil have besked om, når de vises i søgeresultaterne, og du vil blive advaret med en e-mail.

   For eksempel, når 'SEO trends 2019' vises, vil du blive sendt en e-mail med et link videre til det tilsvarende websted. Dette er en fantastisk måde at holde sig opdateret på næsten alt. Derudover kan du begrænse antallet af gange, Google sender e-mails, og få alt pakket ind i en ugentlig oversigt for at undgå et dagligt bombardement.

5. **Gå til YouTube.** I dag er der en video om stort set alt på YouTube. Ja, du skal nogle gange gennemsøge for at finde ædelstenene, men det kan være det værd. Det kan være sådan, at et koncept, du kæmper med, nemt kan løses på få minutter, når du lander på en informativ video.

6. **Brug hashtags.** Dette er en fantastisk måde at søge efter seneste trends, nyheder og opdateringer inden for ethvert felt. Bare brug et par minutter, når du rejser med toget eller under frokosten, for at gå til Twitter eller LinkedIn og søge et par hashtags. Du vil hurtigt kunne navigere til topindholdet under det pågældende hashtag og læse det seneste indhold. Hvis du støder på nogen, der deler regelmæssige opdateringer i din niche, er de nok værd at følge.

5.4.2 Praktiske aktiviteter

Trin 1: Abonner på en YouTube-kanal

1. Gå tilhttps://www.youtube.comi en webbrowser. Dette åbner YouTube-webstedet.

2. Log ind på din konto. Du skal være logget ind på en Google-konto for at abonnere på YouTube-kanaler. Hvis du ikke er logget ind, skal du klikke på den blå "LOG IND"-knap i øverste højre hjørne og derefter logge ind med din Google-konto.

- Hvis du allerede er logget ind og vil skifte konto, skal du klikke på profilbilledet i øverste højre hjørne, vælge Skift konto og derefter vælge en anden konto fra listen. Hvis du ikke kan se den konto, du vil bruge, skal du klikke på Tilføj konto for at tilføje eller oprette en anden konto.

3. Søg efter en kanal.Du kan tjekke, hvad der er Trending, i venstre panel, søge efter en bestemt kanal eller finde noget nyt ved at søge efter søgeord.

- Hvis du kender navnet på den kanal, du vil abonnere på (eller du vil søge efter nøgleord), skal du indtaste det i søgefeltet øverst på YouTube og trykke på Enter eller Retur. For kun at se kanaler skal du klikke på Filtrer i øverste venstre hjørne af søgeresultaterne og vælge Kanaler under "Type".
- Du kan også abonnere på en kanal fra enhver af kanalens videoer. Indtast navnet på en video i søgefeltet, og tryk på Enter eller Retur. Klik derefter på en video for at begynde at se den – kanalens navn vises under videoens titel.

4. Klik på ABONNER for at abonnere på en kanal.Det er en rød-hvid knap – hvis du er på kanalens startside, vil den være tæt på øverste højre hjørne af siden under forsidebilledet. Hvis du har en video åben, er den under videoen til højre for kanalens navn.

- Nu hvor du er tilmeldt, bliver teksten på "ABONNER"-knappen grå og ændres til ABONNERET. Hvis du til enhver tid klikker på den knap, vil du afmelde dig fra kanalen.

5. Se dine abonnementer.Klik på de tre vandrette linjer i øverste venstre hjørne af YouTube for at åbne menuen og vælg Abonnementer for at se alle de kanaler, du abonnerer på.

- Dine abonnementer vises under "ABONERINGER" i panelet til venstre.
- Klik på en af dine abonnenter for at se dens seneste indhold.

6. Juster dine meddelelsespræferencer.Du vil som standard blive underrettet om nogle kanalopdateringer. For at modtage flere eller færre opdateringer fra en kanal skal du klikke på kanalen og derefter klikke på klokkeikonet ved siden af knappen "ABONNER". Klik derefter på Alle, Ingen eller Personligt. Personlig baserer notifikationer på din aktivitet.

- For at angive, hvordan du får besked om opdateringer, skal du klikke på dit profilbillede i øverste højre hjørne, vælge Indstillinger og derefter klikke på Notifikationer i venstre panel. Brug skyderne til at styre, hvilke notifikationer du får besked om.

Trin 2: Deltag i en interessegruppe på sociale medier

1. Åbn Facebook. Facebook-mobilapp-ikonet er et hvidt "f" på en mørkeblå baggrund. Facebook åbner for dit nyhedsfeed, hvis du allerede er logget ind.

- Hvis du ikke allerede er logget ind, skal du indtaste din e-mailadresse (eller telefonnummer) og adgangskode, og derefter trykke på Log ind.

2. Tryk på søgelinjen.Det er øverst på skærmen. Dette vil hente din enheds tastatur frem.

3. Indtast et gruppenavn eller nøgleord. Indtast en gruppes navn (eller et ord eller en sætning, som du er interesseret i), og tryk derefter på Søg. Dette vil søge på Facebook efter konti, sider, steder og grupper, der matcher din søgning.

4. Tryk på Grupper. Dette er en fane nær toppen af skærmen lige under søgefeltet. Dette vil vise alle grupper relateret til din søgning.

- Du skal muligvis stryge rækken af faner her til venstre for at få vist indstillingen Grupper.

5. Tryk på Deltag ved siden af en gruppe.Tilmeld-knappen er på højre side af en gruppes navn. Hvis du trykker på det, vises et "anmodet"-stempel til højre for gruppen. Når du er accepteret i gruppen af en administrator, vil du være i stand til at skrive i gruppen.
Hvis gruppen er offentlig i stedet for lukket, vil du kunne se (men ikke interagere med) gruppens opslag og medlemmer.

Tillykke, du har nu gennemført modul 5 og afsluttet kurset.

Glem ikke at tjekke bilagene for yderligere ressourcer og dokumenter til støtte for selvstudium! Godt klaret!

No One Behind

Co-funded by the Erasmus+ Programme of the European Union

EVALUERING AF UDDANNELSEN

1. Evaluering af læringen

Inden for metodologien for No One Behind-projektet udviklede konsortiet det evalueringssystem, der er behørigt introduceret i dokumentet Innovativ metodologi til at uddanne og træne voksne fra landdistrikterne for at forbedre deres digitale og ikt-færdigheder[19]. I henhold til dette system er der for hver kompetenceenhed defineret de kvalitative indikatorer til vurdering af kompetencedomænet for voksne elever (tabel):

M1 - Information og datafærdighed	
Gennemse, søge og filtrere data, information og digitalt indhold	- Kunne identificere forskellige webbrowsere. - Kunne genkende forskellige søgemaskiner. - Kunne søge information og indhold online. - Kunne navigere mellem digitale miljøer. - Kunne forstå risikoen for fortrolighed og privatliv ved søgning på internettet. - Kunne kende internettets rolle i at indhente information i sammenhæng med nutidens verden.
Evaluering af data, information og digitalt indhold	- Kunne genkende farerne ved falske nyheder og misinformation i den digitale tidsalder. - Kunne identificere rigtigheden af data og nøjagtigheden af digital information. - Kunne opdage troværdigheden og pålideligheden af almindelige datakilder, informationer og deres digitale indhold. - Kunne søge efter pålidelige og troværdige data og informationer.
Håndtering af data, information og digitalt indhold	- Kunne identificere forskellige typer programmer, værktøjer og miljøer til at lagre og administrere data, information og digitalt indhold. - Kunne bruge digitale værktøjer og platforme til at lagre og administrere data. - Kunne organisere indhold og data i en digital platform på en struktureret måde. - Være i stand til at få adgang til digitale miljøer, der definerer passende privatlivsindstillinger.
M2 - Kommunikation og Samarbejde	
Interagere gennem digitale teknologier	- Kunne identificere forskellige digitale værktøjer, karakterisere dem og bruge dem i overensstemmelse med konteksten. - Kunne interagere og kommunikere med forskellige målgrupper ved hjælp af passende digitale værktøjer og enheder. - Kunne genkende og karakterisere forskellige digitale platforme og enheder til kommunikation. - Være i stand til at søge information online på sikkert og etisk forsvarlig vis.
Deling gennem digitale teknologier	- Kunne dele information med andre ved hjælp af passende værktøjer og/eller platforme. - Kunne genkende og karakterisere forskellige digitale platforme og enheder til deling af information. - Kunne dele information med andre på en sikker og etisk måde. - Være i stand til at søge information online på sikkert og etisk forsvarlig vis.
Engagere sig i medborgerskab gennem digitale teknologier	- Kunne kommunikere online etisk og fordomsfrit. - Kunne deltage online i samfundet som borger. - Kunne bruge lovlige onlinetjenester. - Kunne give feedback og meninger med respekt for andre.

[19] Tilgængelig her.

	- Kunne genkende information og interaktive onlinetjenester. - Være i stand til at konfigurere indstillinger for at holde oplysningerne private.
Samarbejde gennem digitale teknologier	- Kunne bruge forskellige værktøjer og platforme til at kommunikere online med andre. - Kunne dele information online ved hjælp af passende værktøjer og platforme. - Kunne identificere de mest brugte online platforme i deres land eller region. - Kunne skelne mellem instant messaging eller chat platforme, voice-over-IP, sociale medie platforme, fora og e-mail.
Netiquette	- Kunne udvise høflig interaktion online med andre. - Kunne identificere, hvilken slags adfærd der skal bruges i forskellige online miljøer (såsom e-mail, sociale medier eller chat). - Kunne anvende "gode manerer" i et online miljø, der kommunikerer med andre. - Kunne forstå vigtigheden af online regler ved brug af digitale ressourcer.
Håndtering af digital identitet	- Kunne beskrive begrebet digital identitet. - Kunne forstå, hvordan man beskytter den digitale identitet. - Kunne beskrive enkle måder at beskytte omdømmet på online. - Kunne styre det digitale fodaftryk. - Kunne vide, hvordan man respekterer andres digitale identiteter og er opmærksom på, hvad man skriver om andre mennesker.
M3 - Oprettelse af digitalt indhold	
Udvikling af digitalt indhold	- Kunne oprette og redigere digitalt indhold i forskellige formater. - Kunne skabe nyt, originalt indhold og viden. - Kunne godt repræsentere, hvad det er hensigten at kommunikere. - Kunne identificere værdien af digitalt indhold som visuelt hjælpemiddel. - Kunne tilpasse udtrykket gennem skabelse af de mest hensigtsmæssige digitale virkemidler.
Integrering og re-udarbejdelse af digitalt indhold	- Kunne ændre information og indhold til et eksisterende dokument eller platform. - Kunne integrere ny information og indhold i et eksisterende dokument eller platform. - Kunne vurdere de mest hensigtsmæssige måder at integrere specifikke nye indholds- og informationselementer på.
Copyright og licenser	- Kunne anvende copyright og licenser på en nøjagtig måde. - Kunne identificere hvilke licenser der kræves under visse omstændigheder. - Kunne vide, hvordan man beskytter sig mod krænkelse af ophavsretten.
Programmering	- Kunne angive simple instruktioner til et computersystem til at løse et simpelt problem eller udføre en simpel opgave. - Kunne løse simple tekniske problemstillinger. - Kunne anvende instruktioner til at udføre opgaver eller løse problemer..
M4 - Sikkerhed	
Beskyttelse af enheder	- Kunne forstå vigtigheden af at beskytte enheder og undgå risici. - Kunne identificere forskellen mellem forskellige typer malware. - Kunne forstå vigtigheden af tiltag relateret til pålidelighed og fortrolighed.

Beskyttelse af personlige data og privatliv	- Være i stand til at holde personlige data beskyttet. - Kunne forstå risikoen for identitetstyveri. - Kunne anvende "Privatlivspolitik" ved brug af digitale tjenester. - Kunne forstå de grundlæggende regler for sikkerhed.
Beskyttelse af sundhed og velvære	- Kunne undgå sundhedsrisici og trusler mod fysisk og psykisk velvære ved brug af digitale teknologier. - Kunne kontrollere mulige farer og trusler i digitale miljøer. - Kunne identificere risici ved misbrug af online og digitale tjenester.
Beskyttelse af miljøet	- Kunne genkende simple miljøpåvirkninger af digitale teknologier og deres anvendelse. - Kunne bruge digitale tjenester uden at være afhængig af dem. - Være i stand til at beskytte miljøet mod påvirkningen fra bortskaffelse af digitale enheder.
M5 - Problemløsning	
Løsning af tekniske problemer	- Kunne navigere på nettet i hverdagssammenhænge. - Kunne identificere, hvornår en digital enhed er passende nok til at arbejde på. - Kunne identificere, hvornår der er opstået et problem på en digital enhed eller tjeneste.
Identificering af behov og teknologiske reaktioner	- Kunne genkende tekniske problemer, der stammer fra en digital enhed eller fra miljøet. - Kunne genkende løsningsmetoder. - Kunne forstå, hvordan man bruger hjælpefaciliteter, manualer guider.
Kreativ brug af digitale teknologier	- Kunne bruge den relevante digitale teknologi til et bestemt formål (indsamle information, skabe indhold). - Kunne bruge komponenter af digitale systemer og digital information under virkelige forhold.
Identificering af digitale kompetencegab	- Kunne vurdere sig selv eller andre, om nye digitale miljøer er hensigtsmæssige midler til at forbedre det digitale kompetenceniveau. - Kunne søge muligheder for selvudvikling og holde sig ajour med den digitale udvikling.

Bord 31 – Identifikation af beviskriterierne for hver kompetenceenhed til vurdering af kompetencedomænet af voksne elever.

Disse beviskriterier bør bruges til at vurdere kompetencedomænet af elever, og det kan vurderes på to måder:

- Af voksenundervisere eller undervisere gennem observation af elevernes præstationer under udviklingen af de foreslåede aktiviteter og ved slutningen af træningen ved at udfylde et evalueringsark.
- Af voksne elever, der vurderer deres kompetencedomæne ved at udfylde et selvevalueringsark i begyndelsen og slutningen af hvert modul.

I begge tilfælde kan det bruges de evalueringsark, der findes i **Bilag II til V.**

2. Evaluering af uddannelsen

I slutningen af uddannelsesforløbet forventes evaluering af det af elever, der har gavn af det. Evalueringen af uddannelsen vil gøre det muligt at forstå:

- træningens tilstrækkelighed og relevans for de definerede målgrupper
- uddannelsespensums kvalitet med hensyn til indhold og varighed
- værdien af støtten og materialerne
- støtte under uddannelsen

Dette vil blive gjort gennem et spørgeskema (bilag VI), der vil være tilgængeligt online. Vi anbefaler også et debriefing-øjeblik i slutningen af hvert modul og i slutningen af kurset, hvor eleverne kan finde plads til at tale om deres læringserfaring, hvad de kunne lide mest og mindst, hvad var deres største vanskeligheder, hvordan de planlægger at blive ved med at praktisere det, de har lært på kurset og så videre.

No One Behind

Co-funded by the Erasmus+ Programme of the European Union

BILAG

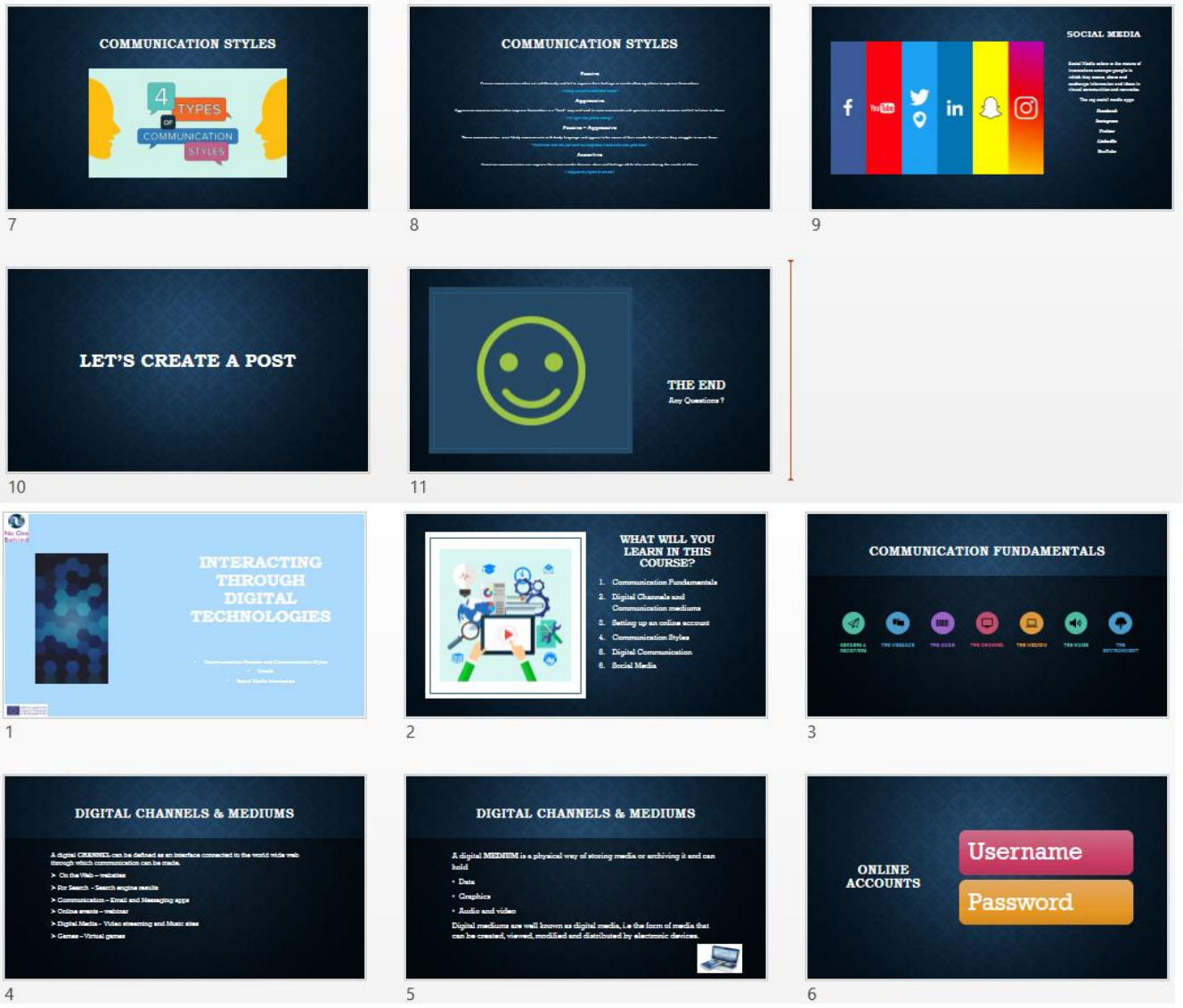
Bilag I – Yderligere ressourcer

modul	Enhed	Ressourcer
Modul 1	1.1	**IT online undervisning** – https://edu.gcfglobal.org/en/subjects/tech/ **Tutorial "Brug af søgemaskiner"** – https://edu.gcfglobal.org/en/internetbasics/using-search-engines/1/ **Sådan søger du effektivt på internettet (1)** – https://mediasmarts.ca/sites/default/files/pdfs/tipsheet/TipSheet_How_Search_Internet_Effectively.pdf **Sådan søger du effektivt på internettet (2)** – https://mediasmarts.ca/sites/default/files/tip-sheet/tipsheet_we_are_broadcasters.pdf
	1.2	**Data beskyttelse** - https://ec.europa.eu/info/sites/default/files/charter-application_en.pdf **Hvordan spredes falske nyheder** - https://www.youtube.com/watch?v=cSKGa_7XJkg
Modul 2	2.1	**Grundlæggende e-mail-vejledning**: https: //www.youtube.com/watch?v=cnxsl8h5gj4 **Brug af digitale værktøjer til at transformere klasseværelser**: https://www.youtube.com/watch?v=B99FXVamqMM **Hvad din digitale kommunikationsstil siger om dig**: https://www.webroot.com/us/en/resources/tips-articles/what-your-digital-communication-style-says-about-you
	2.2	**Bedste lektioner til at dele lektionsnoter digitalt:**http://blog.whooosreading.org/digital-notes/ **Del digitalt og kommenter:** https://applieddigitalskills.withgoogle.com/c/middle-and-high-school/en/create-a-presentation-all-about-a-topic/create-a-presentation-all-about-a-topic/digitalt-del-og-kommenter.html
	2.3	**Digitalt medborgerskab:** https://education.microsoft.com/en-us/course/192d4b4a/overview https://www.youtube.com/watch?v=ju9aOc2MLyo https://www.youtube.com/watch?v=HIll6YjE2ds https://ikeepsafe.org/content/uploads/2020/02/Class-2_Student_FINAL-1.pdf **Hvad er personlige oplysninger:** https://www.commonsensemedia.org/educators/lesson/keep-it-private-k-2 **Digitalt medborgerskab og dets undervisning:** https://files.eric.ed.gov/fulltext/EJ1286737.pdf
	2.4	**30 af de bedste digitale samarbejdsværktøjer til studerende** - https://www.teachthought.com/technology/12-tech-tools-for-student-to-student-digital-collaboration/ **Vigtigheden af teamwork og samarbejde i en digital verden** - https://blog.bit.ai/importance-of-teamwork-and-collaboration/ **Digitalt samarbejdsværktøj**: https://www.youtube.com/watch?v=TSz2CxnuGkQ https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework https://zapier.com/blog/dropbox-vs-google-drive/ https://support.google.com/a/users/answer/9302892?hl=da https://kissflow.com/project/best-project-management-tools/

modul	Enhed	Ressourcer
	2.5	**Netikette betydning, definition og forklaring -** https://www.youtube.com/watch?v=7-HopTAFUm0 **Eksempler på dårlig netiquette -** https://www.cybersmile.org/what-we-do/advice-help/netiquette/examples-of-bad-netiquette **Eksempler på god netiquette -** https://www.cybersmile.org/advice-help/category/examples-of-good-netiquette https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework https://www.cybersmile.org/what-we-do/advice-help/netiquette/examples-of-bad-netiquette https://slangit.com/meaning/keyboard_warrior
	2.6	**Adgangskoder: Sådan beskytter du dine digitale aktiver -** https://www.funeralwise.com/learn/digitallegacy/how-to-manage-passwords/ **Den digitale identitet: hvad det er + hvorfor det er værdifuldt -** https://learn.g2.com/digital-identity **Hvad er digital identitet, og hvordan fungerer det -** https://www.techfunnel.com/information-technology/what-is-digital-identity/ https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework https://www.zdnet.com/article/identity-management-101-how-digital-identity-works/ https://www.techrepublic.com/article/how-to-protect-yourself-and-your-organization-against-digital-identity-fraud/ https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message
Modul 5		https://medium.com/beyond/6-ways-to-stay-on-top-of-emerging-technology-trends-ca6a7b27bc20 https://www.imaginaire.co.uk/16-ways-to-stay-up-to-date-with-digital-marketing-trends-in-2019-our-guide-to-tips-and-resources https://digital-strategy.ec.europa.eu/en/library/digital-skills-gap-europe http://www.dcds-project.eu/wp-content/uploads/2019/02/D6_DCD-Methodology-_v1_revised.pdf http://www.dcds-project.eu/wp-content/uploads/2018/12/D5_Contents_assessment_tool.pdf https://www.digitalhrtech.com/skills-gap-analysis 341727166_Digitale_Kreative_færdigheder_Hvad_er_de_Hvordan_ser_progression_som_Hvordan_er_de_udvikles_Hvad_lovende_praksis_er_der_ https://www.opencolleges.edu.au/informed/features/8-ways-boost-creativity-technology https://www.techwalla.com/articles/why-is-a-file-extension-important https://slidetodoc.com/solving-technical-problems-identifying-needs-and-technological-responses/ https://www.mcafee.com/blogs/consumer/consumer-threat-reports/software-updates-important/

Yderligere ressourcer – Power Point-præsentationer

Modul 2, enhed 2.1 – Interagere gennem digitale teknologier



Modul 2, enhed 2.2 - Deling gennem digitale teknologier

1

2

3

4

5

6

7

8

Modul 2, enhed 2.3 – Engagere sig i medborgerskab gennem digitale teknologier

1

2

3

4

5

6

7

8

9

10

11

12

13

14

Bilag II – Evalueringsark Modul 1. Information og datafærdighed

Information og datafærdighed

1.1. Gennemse, søge og filtrere oplysninger

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne identificere forskellige webbrowsere.	☐	☐	☐
Kunne genkende forskellige søgemaskiner.	☐	☐	☐
Kunne søge information og indhold online.	☐	☐	☐
Kunne navigere mellem digitale miljøer.	☐	☐	☐
Være i stand til at forstå risikoen for fortrolighed og privatliv ved søgning på internettet.	☐	☐	☐
Være i stand til at kende internettets rolle i at indhente information i sammenhæng med nutidens verden.	☐	☐	☐

1.2. Evaluering af data, information og digitalt indhold

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Være i stand til at genkende farerne ved falske nyheder og misinformation i den digitale tidsalder.	☐	☐	☐
Kunne identificere rigtigheden af data og nøjagtigheden af digital information.	☐	☐	☐
Være i stand til at opdage troværdigheden og pålideligheden af almindelige datakilder, informationer og deres digitale indhold.	☐	☐	☐
Kunne søge efter pålidelige og troværdige data og informationer.	☐	☐	☐

1.3. Håndtering af data, information og digitalt indhold

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne identificere forskellige typer programmer, værktøjer og miljøer til at lagre og administrere data, information og digitalt indhold.	☐	☐	☐
Kunne bruge digitale værktøjer og platforme til at lagre og administrere data.	☐	☐	☐
Kunne organisere indhold og data i en digital platform på en struktureret måde.	☐	☐	☐
Være i stand til at få adgang til digitale miljøer, der definerer passende privatlivsindstillinger.	☐	☐	☐

Bilag III – Evalueringsark Modul 2. Kommunikation og samarbejde

Kommunikation og samarbejde

2.1. Interagere gennem teknologier

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne identificere forskellige digitale værktøjer, karakterisere dem og bruge dem i overensstemmelse med konteksten.	☐	☐	☐
Være i stand til at interagere og kommunikere med forskellige målgrupper ved hjælp af passende digitale værktøjer og enheder.	☐	☐	☐
Kunne genkende og karakterisere forskellige digitale platforme og enheder til kommunikation.	☐	☐	☐
Være i stand til at søge efter information online på en sikker og etisk måde.	☐	☐	☐

2.2. Deling gennem digitale teknologier

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne dele information med andre ved hjælp af passende værktøjer og/eller platforme.	☐	☐	☐
Kunne genkende og karakterisere forskellige digitale platforme og enheder til deling af information.	☐	☐	☐
Være i stand til at dele information med andre på en sikker og etisk måde.	☐	☐	☐
Være i stand til at søge efter information online på en sikker og etisk måde.	☐	☐	☐

2.3. Engagere sig i medborgerskab gennem digitale teknologier

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne kommunikere online etisk og fordomsfrit.	☐	☐	☐
Kunne deltage online i samfundet som borger.	☐	☐	☐
Kunne bruge lovlige onlinetjenester.	☐	☐	☐
Kunne give feedback og meninger med respekt for andre.	☐	☐	☐
Kunne genkende information og interaktive onlinetjenester.	☐	☐	☐
Være i stand til at konfigurere indstillinger for at holde oplysningerne private.	☐	☐	☐

2.4. Samarbejde gennem digitale teknologier

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne bruge forskellige værktøjer og platforme til at kommunikere online med andre.	☐	☐	☐
Være i stand til at dele information online ved hjælp af passende værktøjer og platforme.	☐	☐	☐
Være i stand til at identificere de mest brugte online platforme i deres land eller område.	☐	☐	☐
Være i stand til at skelne mellem instant messaging eller chat platforme, voice-over-IP, sociale medie platforme, fora og e-mail.	☐	☐	☐

2.5. Netiquette			
Kompetenceenhed	**Ingen**	**Grundlæggende**	**Over Basic**
Være i stand til at demonstrere høflig interaktion online med andre.	☐	☐	☐
Kunne identificere, hvilken slags adfærd der skal bruges i forskellige online miljøer (såsom e-mail, sociale medier eller chat).	☐	☐	☐
Være i stand til at anvende "gode manerer" i et online miljø, der kommunikerer med andre.	☐	☐	☐
Kunne forstå vigtigheden af online regler ved brug af digitale ressourcer.	☐	☐	☐
2.6. Håndtering af digital identitet			
Kompetenceenhed	**Ingen**	**Grundlæggende**	**Over Basic**
Kunne beskrive begrebet digital identitet.	☐	☐	☐
Kunne forstå, hvordan man beskytter den digitale identitet.	☐	☐	☐
Kunne beskrive enkle måder at beskytte omdømmet på online.	☐	☐	☐
Kunne styre det digitale fodaftryk.	☐	☐	☐
Være i stand til at vide, hvordan man respekterer andres digitale identiteter og er opmærksom på, hvad man skriver om andre mennesker.	☐	☐	☐

Bilag IV – Evalueringsark Modul 3. Indholdsskabelse

Oprettelse af digitalt indhold

3.1. Udvikling af indhold

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne oprette og redigere digitalt indhold i forskellige formater.	☐	☐	☐
Kunne skabe nyt, originalt indhold og viden.	☐	☐	☐
Kunne godt repræsentere, hvad det er hensigten at kommunikere.	☐	☐	☐
Kunne identificere værdien af digitalt indhold som visuelt hjælpemiddel.	☐	☐	☐
Kunne tilpasse udtrykket gennem skabelsen af de mest hensigtsmæssige digitale virkemidler.	☐	☐	☐

3.2. Integrering og re-uddybning

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Være i stand til at ændre information og indhold til et eksisterende dokument eller platform.	☐	☐	☐
Være i stand til at integrere ny information og indhold i et eksisterende dokument eller platform.	☐	☐	☐
Være i stand til at vurdere de mest hensigtsmæssige måder at integrere specifikke nye indholds- og informationselementer på.	☐	☐	☐

3.3. Copyright og licenser

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Være i stand til at anvende copyright og licenser på en nøjagtig måde.	☐	☐	☐
Være i stand til at identificere, hvilke licenser der kræves under visse omstændigheder.	☐	☐	☐
Kunne vide, hvordan man beskytter sig mod krænkelse af ophavsretten.	☐	☐	☐

3.4. Programmering

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne angive simple instruktioner til et computersystem til at løse et simpelt problem eller udføre en simpel opgave.	☐	☐	☐
Kunne løse simple tekniske problemstillinger.	☐	☐	☐
Kunne anvende instruktioner til at udføre opgaver eller løse problemer.	☐	☐	☐

Bilag IV – Evalueringsark Modul 4. Sikkerhed

Sikkerhed

4.1. Beskyttelse af enheder

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne forstå vigtigheden af at beskytte enheder og undgå risici.	☐	☐	☐
Kunne identificere forskellen mellem forskellige typer malware.	☐	☐	☐
Kunne forstå vigtigheden af tiltag relateret til pålidelighed og fortrolighed.	☐	☐	☐

4.2. Beskyttelse af personlige data

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Være i stand til at beskytte personlige data.	☐	☐	☐
Kunne forstå risikoen for identitetstyveri.	☐	☐	☐
Kunne anvende "Privatlivspolitik" ved brug af digitale tjenester.	☐	☐	☐
Kunne forstå de grundlæggende regler for sikkerhed.	☐	☐	☐

4.3. Beskyttelse af sundhed

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne undgå sundhedsrisici og trusler mod fysisk og psykisk velvære ved brug af digitale teknologier.	☐	☐	☐
Kunne kontrollere mulige farer og trusler i digitale miljøer.	☐	☐	☐
Kunne identificere risici ved misbrug af online og digitale tjenester.	☐	☐	☐

4.4 Beskyttelse af miljøet

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne genkende simple miljøpåvirkninger af digitale teknologier og deres anvendelse.	☐	☐	☐
Kunne bruge digitale tjenester uden at være afhængig af dem.	☐	☐	☐
Være i stand til at beskytte miljøet mod påvirkningen fra bortskaffelse af digitale enheder.	☐	☐	☐

Bilag V – Evalueringsark Modul 5. Problemløsning

Problemløsning

5.1. Løsning af tekniske problemer

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne navigere på nettet i hverdagssammenhænge.	☐	☐	☐
Kunne identificere, hvornår en digital enhed er passende nok til at arbejde på.	☐	☐	☐
Kunne identificere, hvornår der er opstået et problem på en digital enhed eller tjeneste.	☐	☐	☐

5.2. Identificering af behov og teknologiske reaktioner

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne genkende tekniske problemer, der stammer fra en digital enhed eller fra miljøet.	☐	☐	☐
Kunne genkende løsningsmetoder.	☐	☐	☐
Kunne forstå, hvordan man bruger hjælpefaciliteter, manualer guider.	☐	☐	☐

5.3. Innovation og kreativ brug af teknologi

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne bruge den relevante digitale teknologi til et bestemt formål (indsamle information, skabe indhold).	☐	☐	☐
Kunne bruge komponenter af digitale systemer og digital information under virkelige forhold.	☐	☐	☐

5.4. Identificering af digitale kompetencegab

Kompetenceenhed	Ingen	Grundlæggende	Over Basic
Kunne vurdere sig selv eller andre, om nye digitale miljøer er hensigtsmæssige midler til at forbedre det digitale kompetenceniveau.	☐	☐	☐
Kunne søge muligheder for selvudvikling og holde sig ajour med den digitale udvikling.	☐	☐	☐

Bilag VI – Evaluering af uddannelsen

Dette evalueringsark har som hovedformål at indsamle data og din feedback om kvaliteten af uddannelsesprogrammet for en "digital kompetent" borger. Dette spørgeskema skal udfyldes individuelt og ved afslutningen af uddannelsen. Spørgeskemaet er fortroligt, og din mening er afgørende for forbedringen af træningsprogrammet.
Spørgeskemaet er opbygget i tre dele: Del A – Statistik har to spørgsmål, der giver partnerne mulighed for at lave en statistisk analyse af de gennemførte workshops; del B - Kvantitativ evaluering er sammensat af 13 udsagn, der skal besvares med følgende skala fra 1 til 5: 1 - meget uenig, 2 - for det meste uenig, 3 - Hverken enig eller uenig, 4 - for det meste enig og 5- meget enig[20]; del B – Kvalitativ evaluering er sammensat af to åbne spørgsmål: et første, hvor du skal komme med yderligere kommentarer/forslag til de udsagn, du scorede med 1, 2 eller 3; en anden, hvor du kan tilføje yderligere kommentarer til træningsprogrammet og workshoppen.

Del A – Personlige data

Bopælsland

Rumænien ☐ Portugal ☐ Grækenland ☐ Italien ☐ Danmark ☐

Erhverv

Del B – Kvantitativ evaluering

	1	2	3	4	5	NA
Uddannelsesplanen er relevant for mit personlige og/eller professionelle liv.						
Uddannelsen svarede til mine oprindelige forventninger.						
Målene for uddannelsen blev nået.						
De behandlede enheder og indhold var interessante og relevante.						
Uddannelsens varighed er i henhold til dens mål, indhold og aktiviteter/opgaver.						
Uddannelsen gav mulighed for at tilegne sig digitale kompetencer.						
Indholdet, praksis og/eller instrumenter introduceret i træningen var egnede til at blive implementeret i mine daglige aktiviteter.						
De støttematerialer, der blev brugt under uddannelsen, var tilstrækkelige (med hensyn til design, sprog, brugbarhed, givet information).						
De aktiviteter, opgaver og øvelser, der foreslås under uddannelsen, er tilstrækkelige til tilegnelse og udvikling/konsolidering af digitale kompetencer.						
Underviserne ydede den nødvendige støtte til deltagerne under træningen.						
Underviserne var tydelige og effektive under træningen.						
Underviserne fremmede deltagernes deltagelse og involvering i træningen.						

Del C – Kvalitativ evaluering

[20] Hvis en af udsagnene ikke gælder for din oplevelse, bedes du svare "NA" (Ikke relevant).

1. Angiv venligst yderligere anbefalinger/forslag vedrørende udsagnet, som du scorede med 1, 2 eller 3:

2. Har du yderligere kommentarer til uddannelsesplanen? Del det gerne her.

Dato: ___ / ____ / _____

Tak for dit bidrag!

No One Behind

Co-funded by the Erasmus+ Programme of the European Union

REFERENCER

Europa-Kommissionen: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en

Celebic, G. & Rendulic, D. (2011). Grundlæggende begreber i informations- og kommunikationsteknologihåndbog. Open Society for Idea Exchange (ODRAZI), Zagreb. Kilde:http://www.itdesk.info/handbook_basic_ict_concepts.pdf

Encyclopaedia Britannica: https://www.britannica.com/technology/browser

Australian Cyber Security Center: https://www.cyber.gov.au/acsc/view-all-content/guidance/proactive-measures-protect-your-information

Georgetown Universitetsbibliotek: https://www.library.georgetown.edu/tutorials/research-guides/evaluating-internet-content

Smithsonian Magazine: https://www.smithsonianmag.com/science-nature/what-emotion-goes-viral-fastest-180950182/?no-ist

Washington State University Vancouver: https://webliteracy.pressbooks.com/chapter/building-a-habit-by-checking-your-emotions/#footnote-51-1

Balancen lille virksomhed: https://www.thebalancesmb.com/copyright-definition-2948254

Universitet, Spring Arbor. Grundlæggende kommunikation: 8 grundlæggende begreber og definitioner. Spring Arbor University. [Online] juni 2021. https://online.arbor.edu/news/fundamentals-communication-eight-basic-concepts-and-definitions.

7 Eksempler på digitale kanaler. **Spacey, John.** 2017, Forenklet.

De 10 nye kommunikationsparadigmer i den digitale tidsalder. **Orihuela, Jose Luis.** 2017, Jlori.

4 typer kommunikationsstile. Alvernia Universitet. Pennsylvania: sn, 2018, Alvernia University, s. 2.

LEADGENERA.LEADGENERA. Content Marketing. [Online] juni 2021. https://leadgenera.com/knowledge-hub/marketing/the-10-best-social-media-and-content-apps-for-2020/.

Kommissionen, europæisk. Den digitale kompetenceramme 2.0. EU SCIENCE HUB. [Online] 9. januar 2019. https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework.

Omsorg, Institut for Sundhed og Social. Engagere. Digitalt pas. [Online] https://engage.dhsc.gov.uk/digitalpassport/tools/.

Google. Google. Google Drev. [Online] Google. https://support.google.com/drive/answer/2424384?hl=da&co=GENIE.Platform%3DDesktop.

Europa-Kommissionen. Europa. Transformation af digitalt medborgerskab. [Online] Europa-Kommissionen. https://epale.ec.europa.eu/en/blog/digital-citizenship-transformation.

Sund fornuft. Alt hvad du behøver for at lære digitalt medborgerskab. [hjemmeside] sl : Common Sense, 2021.

australske regering.eSafety Commissioner. Digital Borgervejledning. [Online] https://www.esafety.gov.au/media/2563.

Liveworkstudio.leve|arbejde. Digitale relationer. [Online] https://www.liveworkstudio.com/themes/organisational-change/digital-relationships/.

Eferin, Kate Gromova og Yaroslav. Verdensbankens blogs. Etik i den digitale verden: Hvor er vi nu, og hvad er det næste. [Online] 9. april 2021. https://blogs.worldbank.org/opendata/ethics-digital-world-where-we-are-now-and-whats-next.

Zwierdling, Daniel. npr. Dit digitale spor, og hvordan det kan bruges mod dig. [Online] 2013. https://www.npr.org/sections/alltechconsidered/2013/09/30/226835934/your-digital-trail-and-how-it-can-beused-against-you.

University of Alabama i Birmingham.UAB Institute for Human Rights Blog. Digitalt medborgerskab: Det gode, det dårlige og internettets rolle. [Online] Januar 2019. https://sites.uab.edu/humanrights/2019/01/18/digital-citizenship-the-good-the-bad-the-role-of-the-internet/.

BYU bibliotek:

- https://guides.lib.byu.edu/c.php?g=216340&p=1428402
- https://www.techwalla.com/articles/why-is-a-file-extension-important
- https://slidetodoc.com/solving-technical-problems-identifying-needs-and-technological-responses/
- https://www.mcafee.com/blogs/consumer/consumer-threat-reports/software-updates-important/
- https://www.opencolleges.edu.au/informed/features/8-ways-boost-creativity-technology/

No One Behind

Co-funded by the Erasmus+ Programme of the European Union

Dette projekt er blevet finansieret med støtte fra Europa-Kommissionen. Denne publikation afspejler kun forfatterens synspunkter, og Kommissionen kan ikke holdes ansvarlig for enhver brug, der kan gøres af oplysningerne deri.

Projekt n. º 2020-1-RO01-KA204-079988