CYBERMISSIONEN

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING

CYBER SKILLS

CYBERMISSIONEN 2023 LÆRER

ISBN nr:
87-603-3350-2 (web udgave)

Design:
Børne- og
Undervisningsministeriet

Børne- og Undervisningsministeriet
Styrelsen for It og Læring
Teglholmsgade 1
2450 Kbh. SV

Indholdsfortegnelse

I dette materiale, vil der være links og henvisninger til digitale ressourcer og videomateriale, som er tilknyttet Cybermissionen. I det digitale materiale, som ligger på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/ vil alle henvisninger og videoer være klikbare og lette for dig og dine elever at finde.

MISSION 1: UDFORSK DILEMMAERNE VED BRUG AF KUNSTIG INTELLIGENS I EN DIGITAL HANDELSVIRKSOMHED

PRÆSENTATION AF DENNE MISSION

Velkommen til cybermissionen! I denne mission skal I hjælpe virksomheden **SneakPeak** med at implementere ChatGPT i deres kundeservice og markedsføring!

PRÆSENTATION AF CASEVIRKSOMHEDEN

Webshoppen SneakPeak forhandler speciallavede sneakers online. Kunden kan selv bestemme model, farve og materiale, hvorefter SneakPeak laver et par sneakers ud fra kundens design. Virksomheden sælger størstedelen af deres varer i Danmark og deres målgruppe er mellem 15-25 år. SneakPeaks ejer Line vil gerne bruge ChatGPT som et arbejdsværktøj i virksomheden, men ved ikke helt, hvordan de skal komme i gang, og om der vil være ulemper ved at bruge ChatGPT. Hun og resten af SneakPeak har derfor brug for jeres hjælp til at komme i gang.

Virksomheden får rigtig mange henvendelser fra kunder. Cirka halvdelen spørger om generelle ting som farver, størrelser, lagerstatus og leveringstider, mens den anden halvdel har spørgsmål til deres eget design eller deres egen ordre. Størstedelen af kundehenvendelserne kommer efter kl. 18 i hverdagene og i weekenderne, hvor kontoret er lukket. Det betyder, at der hver morgen og særligt om mandagen ligger en stor bunke af kundehenvendelser, der skal besvares. Line vil gerne have bragt svartiden ned, så kunderne får svar på deres spørgsmål så hurtigt som muligt, og allerhelst med det samme. Mange af kundehenvendelserne drejer sig om konkrete ordrer. Det betyder, at SneakPeak har oplysninger om kundernes personoplysninger såsom navn, adresse, nummer og mail liggende i deres systemer.

SneakPeak er begyndt at få en del kunder i Tyskland, og vil derfor gerne udvide deres webshop til det tysktalende marked. Virksomheden vil derfor gerne have oversat deres hjemmeside og alle produktbeskrivelserne til tysk. Virksomheden har mange produkter og beskrivelser på deres webshop, så det er derfor en stor opgave at få oversat det hele til tysk. Den øgede interesse fra Tyskland betyder også, at flere af kundehenvendelserne er på tysk. Medarbejderen Anne, der tager sig af kundehenvendelser og produktbeskrivelser til hjemmesiden, er ikke så skarp til tysk og hun bruger derfor lang tid på at svare på de tyske kundehenvendelser.

Medarbejderen Morten arbejder med virksomhedens sociale medier. Han skriver bl.a. nyhedsbreve og opslag på virksomhedens Instagramprofil. Morten synes, at hans opslag er begyndt at minde for meget om hinanden, og kunne derfor godt bruge lidt inspiration til tekster og indhold til nyhedsbreve.

I denne mission skal I hjælpe Line og resten af SneakPeaks medarbejdere med at komme i gang med ChatGPT. Jeres resultater skal I præsentere for virksomheden i slutningen af forløbet.

Men først skal vi blive lidt klogere på, hvad ChatGPT egentlig er.

PRÆSENTATION AF EKSPERTER

Du vil undervejs i missionen se videoer med to eksperter. Begge eksperter ved rigtig meget om emnet, og arbejder med det til dagligt. I videoerne herunder vil de to eksperter give dig en kort introduktion til dem selv.

Video 01: Introduktion til ekspert - Maria Skjærven
https://cybermissionen.cyberskills.dk/videomateriale2023/

Video 02: Introduktion til ekspert - Emilie Lundblad
https://cybermissionen.cyberskills.dk/videomateriale2023/

HVAD ER GENERATIV AI OG HVOR BLIVER DET BRUGT I DAG?

Først skal vi have styr på, hvad generativ AI er. AI står for "Artificial Intelligence", som på dansk hedder kunstig intelligens.

Emilie vil herunder give dig en kort introduktion til, hvad kunstig intelligens handler om.

Video 03: Hvad er kunstig intelligens
https://cybermissionen.cyberskills.dk/videomateriale2023/

Emilie nævner *"Machine Learning"*, som også kaldes maskinlæring på dansk. Maskinlæring er, når vi mennesker lærer en maskine at gøre noget, som ellers vil kræve, at et menneske gjorde det. Et eksempel på det er, når du handler på en webshop. Du har måske prøvet at se på en vare og også fået andre varer med overskriften "Måske du også er interesseret i disse varer". Det kan maskinen foreslå dig, fordi den er blevet trænet til at genkende mønstre i, hvilke andre varer kunden typisk også er interesseret i.

Kunstig intelligens kan både være mere simple ting, som webshopeksemplet herover eller når du bruger din GPS til at vise dig vej, men det kan også være meget indviklet og komplekst, som ved generativ AI. Maria fortæller i videoen herunder, hvad generativ AI er.

Video 04: Hvad er generativ AI?
https://cybermissionen.cyberskills.dk/videomateriale2023/

ChatGPT hører ind under betegnelsen generativ AI, da du kan få robotten til at skabe ny tekst til dig. Maria fortæller også om lyd, videoer og billeder, men til disse ting, skal man bruge nogle andre værktøjer end gratisversionen af ChatGPT.

Det vil Maria fortælle mere om her.

Video 05
https://cybermissionen.cyberskills.dk/videomateriale2023/

Overvej: Kan du allerede nu komme med forslag til, hvordan ChatGPT kan hjælpe SneakPeaks medarbejdere?

SNEAKPEAK
STEP UP YOUR STYLE

"

Har du lagt mærke til **SneakPeak-logoet** i starten af missionen? Det er lavet med hjælp fra generative AI-værktøjer. SneakPeak findes slet ikke, men er en virksomhed, vi har opdigtet. Vi har bedt ChatGPT om at give ideer til et navn på en virksomhed, der sælger sneakers. Den kom med en masse forslag, hvor vi valgte at gå videre med navnet SneakPeak. Det er et eksempel på, hvordan ChatGPT også er rigtig god til at hjælpe med at idegenerere. Nu havde vi et navn, men manglede et logo. Der brugte vi et andet kunstig intelligens-værktøj til at hjælpe os med, som kun kan lave billeder – smart, ikke?

ChatGPT kunne kun komme op med et virksomhedsnavn fordi vi fortalte den, hvilken type virksomhed, der var tale om. På den måde kunne den skabe nyt indhold ud fra den information, vi gav den. Jo bedre en kommando vi giver ChatGPT, jo bedre et svar får vi fra den.

➔ **Generativ AI** betyder, at man får en maskine/robot til at generere – altså skabe noget nyt unikt indhold ud fra det information, man har givet den.

➔ **ChatGPT** er et tekstværktøj, som skaber nyt original tekst ud fra den tekst, man skriver til den.

ER ChatGPT DIN NYE KOLLEGA ELLER KONKURRENT?

ChatGPT kan hjælpe dig med opgaver, som er baseret på tekst. I et virksomhedsperspektiv kan det være at skrive nyhedsbreve, opslag på sociale medier, lave kundetilfredshedsundersøgelser, skrive mails, udarbejde produkttekster eller lave søgemaskineoptimering til hjemmesider, så man kommer højere op på Google. Derudover kan man også bruge ChatGPT til at skrive med kunder – du har måske før prøvet at skrive med en Chatbot på en hjemmeside? ChatGPT er trænet på en enorm mængde data, og er udviklet til at kunne føre samtaler med brugeren, så den er markant mere avanceret end en typisk Chatbot. Mulighederne er endeløse, og det kun er fantasien, der sætter grænsen.

Men nu, hvor den kan hjælpe virksomhederne med alle de her opgaver, er der så brug for os mennesker? Ja, det kan du tro! ChatGPT og de andre generativ AI-værktøjer har ikke en menneskelig forståelse ligesom os. Som du allerede har hørt vores eksperter fortælle, baserer ChatGPT sine svar på, hvad den tror er mest sandsynligt, er det rigtige svar. Hvis du spørger den om noget, som den ikke har data på, vil den begynde at digte. Med andre ord – DEN GÆTTER!

Der er ingen tvivl om, at generativ AI, herunder ChatGPT, er kommet for at blive. Men det betyder, at der er brug for medarbejdere, der forstår hvordan de fungerer og kan vurdere, hvilke opgaver der giver god mening at bruge værktøjet til, og endnu vigtigere – hvornår de ikke egner sig. Nogle jobfunktioner vil på sigt blive overtaget af en generativ AI, men det vil også skabe helt nye arbejdsopgaver, som slet ikke findes lige nu.

ChatGPT kommer til at kunne hjælpe rigtig mange virksomheder med at optimere arbejdsprocesser, så medarbejderne kan bruge deres tid på mere komplekse opgaver. Men når virksomheder bare begynder at "lege" med ChatGPT uden at have en forståelse for, hvad det kan og hvad man skal være opmærksom på, kan det gå rigtig galt. Emilie vil fortælle dig om, hvordan virksomheden Samsung har brændt nallerne.

Video 06: Er det gået galt for virksomheder, der har brugt ChatGPT?
https://cybermissionen.cyberskills.dk/videomateriale2023/

Det er vigtigt altid at huske på, at den information og data, du deler med ChatGPT ejes af virksomheden bag, der hedder OpenAI. Derudover bliver det offentlig tilgængeligt. Man kan desuden ikke få slettet sin data igen, hvis man har fundet ud af, at man er kommet til at dele personfølsomme oplysninger eller virksomhedshemmeligheder, ups...

En tommelfingerregel er, at du ikke skal dele noget med ChatGPT, som du ikke vil have liggende på nettet.

DATAETIK

Hvorfor er det vigtigt at vide noget om dataetik, når vi snakker om ChatGPT? ChatGPT er bygget på data, og al den information du giver den, er også data. I forhold til ChatGPT handler dataetik om, at vi skal indsamle, bearbejde og anvende den data vi både giver og får fra ChatGPT på en ansvarlig, kritisk og reflekteret måde.

Vil du være sikker på, at du bruger ChatGPT på en dataetisk måde, som ikke skader hverken dig, din virksomhed eller virksomhedens kunder, så er der her en tjekliste du kan følge. Kan du sætte et flueben ud for dem alle, bruger du ChatGPT på en god måde.

- ☐ **Der må ikke** være personfølsomme eller fortrolige virksomhedsoplysninger i de data, som du deler med ChatGPT (det kræver i så fald samtykke).
- ☐ **Del kun information**, som er nødvendig for at Chat-GPT kan hjælpe dig med at løse opgaven.
- ☐ **Vær kritisk**, hvis du bruger ChatGPT til fortolkning. ChatGPT er nemlig trænet på data, der går langt tilbage, så den kan desværre godt komme med svar der er diskriminerende eller fordomsfulde.
- ☐ **Brug ikke** ChatGPT til at træffe beslutninger uden et menneske har været med indover.
- ☐ **Vær gennemsigtig** over for virksomhedens kunder, hvis de taler med en robot. Det er vigtigt, at kunden ved, at det ikke er et levende menneske, de chatter med.
- ☐ **Test de svar**, som ChatGPT kommer med. Som du allerede nu ved, baserer ChatGPT sine svar udelukkende på, hvad den statistisk set tror, er det rigtige svar. Dens svar kan derfor godt være forkerte eller misvisende. Forholder vi os ikke kritiske til de svar den kommer med, risikerer vi at sprede fake news – altså falsk information.

I videoen herunder vil Maria fortælle dig mere om, hvilke etiske problemstillinger, virksomheder skal være opmærksomme på, hvis de beslutter sig for at erstatte mennesker med en kunstig intelligens.

Video 08: Hvilke etiske problemstillinger er der ved at virksomheder erstatter servicemedarbejdere?
https://cybermissionen.cyberskills.dk/videomateriale2023/

HUSK, hvis noget er gratis, er du eller virksomheden selv produktet

Nogle virksomheder vælger at investere penge i at få udviklet deres egen mini-version af ChatGPT, som kun bliver fodret med data omkring dem. Men hvad er fordelene ved, at virksomheden investerer i sådan en løsning? Det vil Emilie fortælle dig om i denne video:

Video 07: Er der forskel på om man får udviklet sin egen chatbot eller om man bruger ChatGPT?'
https://cybermissionen.cyberskills.dk/videomateriale2023/

Overvej: Hvad er der af fordele og ulemper ved, at en virksomhed bruger ChatGPT til kundeservice frem for at få udviklet deres egen Chatbot.

RISIKOVURDERING

Inden du lader ChatGPT hjælpe dig eller en virksomhed, skal du lave en vurdering af, hvilke risici der følger med, når ChatGPT bliver brugt.

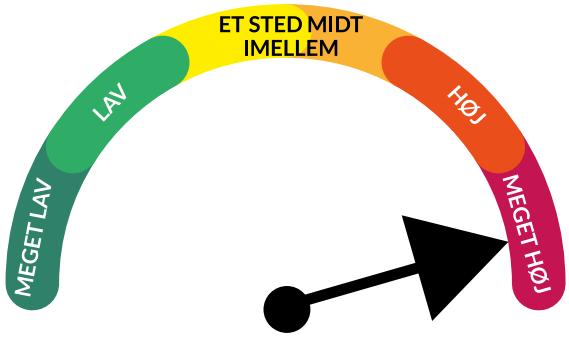
Når man skal lave en risikovurdering, reflekterer man over, hvilke typer af data, ChatGPT skal have for at kunne hjælpe med at løse opgaven eller hvor stor en konsekvens dens svar kan have i en given situation fx for en kunde. Det kan være svært at sige, om der er en lav eller høj risiko forbundet med at inddrage ChatGPT. Følger du tjeklisten fra før, da du læste om dataetik, bevæger du dig i retningen af lav risiko.

Der er altid risici forbundet med at bruge ChatGPT, da vi ikke har fuld kontrol over, hvad der sker med vores data.

Bruger man ChatGPT til fx idegenerering eller til at udarbejde markedsføringstekster, er det begrænset, hvor meget data ChatGPT skal bruge. Skal ChatGPT derimod hjælpe dine kunder med service – det kunne være, hvor langt deres ordre er, vil det kræve at ChatGPT har data på kunden og ordren. Det er langt mere følsomt data, end hvis du skulle have inputs til et nyhedsbrev, hvor du giver ChatGPT information om din virksomhed, som allerede står på jeres hjemmeside.

Forestil dig, at du brugte ChatGPT til at oversætte en jobkontrakt, hvor der blandt andet stod et CPR-nummer og løn. Det er ikke særlig fedt for den pågældende person at have den slags information til at ligge offentlig tilgængelig bagefter.

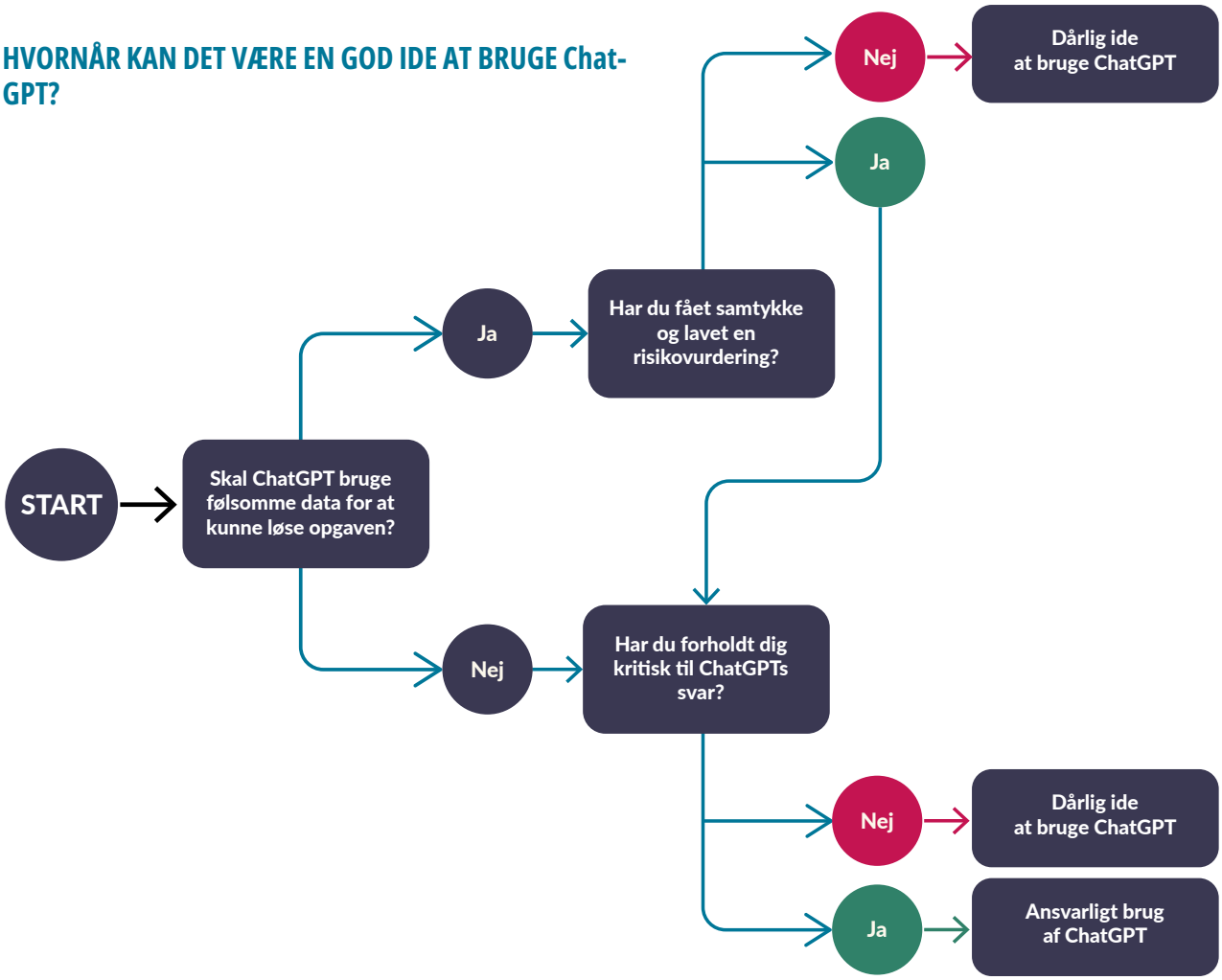
Risikobarometeret nedenfor, kan du bruge som en visuel hjælp. Den kan du bruge, når du skal vurdere, hvor lav eller høj en risiko, der er forbundet med at bruge ChatGPT til at optimere de opgaver, som jeres gruppe vil anbefale SneakPeak at gå i gang med. Husk, at I som gruppe skal kunne argumentere for, hvorfor I har placeret opgaven på barometeret som I har.



Der er nødvendigvis ikke noget galt med at bruge ChatGPT til en opgave med en høj grad af risiko, så længe virksomheden og de involverede medarbejdere forstår at bruge teknologien etisk ansvarligt og tager deres forhåndsregler. Har man ikke arbejdet med ChatGPT før, er det en god idé først at bruge det til at løse lavrisikoopgaver, inden man begiver sig ud i de mere højrisikofyldte, hvor fejlhåndtering af data kan have store konsekvenser.

Det kan være vanskeligt at sætte to streger under, hvornår det er en god idé at gøre brug af ChatGPT og hvornår det er en dårlig idé. Du kan dog bruge illustrationen herunder som en guideline, hvis du er i tvivl.

HVORNÅR KAN DET VÆRE EN GOD IDE AT BRUGE Chat-GPT?



OBS! Der er flere faktorer der kan have indflydelse på, hvorvidt det kan være en god eller dårlig idé at bruge ChatGPT. Denne illustration er blot et eksempel.

PRÆSENTATION

I skal nu lave en præsentation til virksomheden SneakPeak. Tag udgangspunkt i de overvejelser, I har gjort jer gennem forløbet.

Præsentationen skal vare ca. 5-10 min. Og skal indeholde følgende:

- En kort forklaring af, hvad generativ AI er.
- En præsentation af hvor og hvordan SneakPeak kan bruge ChatGPT.
  - Kom gerne med konkrete eksempler
  - Her skal I også komme ind på, hvilke risici der er forbundet med jeres anbefalinger.
- En plan over hvilke opgaver, der skal løses hvornår.

MISSION 2: CYBER AWARENESS

Mange unge oplever, at de har godt styr på deres adfærd på nettet, at de ved, hvad de skal sige ja og nej til, hvad de skal undgå at klikke på, og hvad de generelt skal undgå af fælder - måske tænker du det samme? Men flere undersøgelser viser, at mange ikke altid gør det, de godt ved, de burde gøre i forhold til datasikkerhed.
Det er faktisk ikke kun unge, der mangler viden om datasikkerhed og har brug for en bedre digital adfærd. Det er også et af de områder, som er i fokus hos danske virksomheder: At styrke medarbejdernes viden om, hvordan man agerer sikkert på nettet.

Den udfordring skal I hjælpe med at løse!

VIGTIGHEDEN AF IT-SIKKERHED

De it-løsninger, vi bruger til dagligt, skal helst bare virke, gerne hurtigt, allerhelst uden bøvl og alt for mange krav når man skal oprette konti, logge ind osv. Men sikkerhed betyder også, at det nogle gange bliver besværligt.

For mange er det svært at forstå, hvor stor faren er på nettet, når vi bruger digitale løsninger. Vi kan nemlig ikke altid se de konsekvenser, som 'små handlinger' kan lede til.

It-sikkerhed er et vigtigt område, der skal mere fokus på, og det er det, som I skal arbejde med på denne mission. På denne mission bliver I mestre i god digital adfærd, og så skal I overbevise andre om, at de også skal være opmærksomme på deres it-sikkerhed!

JERES MISSION

I jeres gruppe skal I udvikle en kommunikationskampagne, der henvender sig til målgruppen unge i alderen 15-25 år. I må gerne snævre målgruppen endnu mere ind.

Nedenfor finder I tre aktuelle temaer, som kan være omdrejningspunktet for jeres kommunikationskampagne. I kan bruge én eller flere eller selv komme på en tematik. Det vigtigste er, at kommunikationskampagnen kan forbedre målgruppens digitale adfærd - med fokus på it-sikkerhed. Når I har lavet en kampagne, skal I også forberede en kort præsentation, hvor I fortæller om tankerne bag.

TEMA 1

STYRK DIT PASSWORD

I skal få målgruppen til at lave bedre passwords og passe godt på dem.
De fleste laver forudsigelige passwords, der er lette at gætte/hacke, bruger det samme password til facebook og e-mail m.m. og deler det også med andre, når de eksempelvis låner deres Netflix-konto ud.

TEMA 2

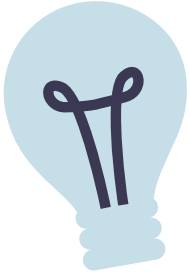
HUSK AT LÅSE DIN COMPUTER

I skal få målgruppen til altid at låse deres computer, når de forlader den.
Hvor tit har I ikke forladt jeres plads uden at låse jeres computer? Det sker alt for tit, og I skal derfor gøre målgruppen opmærksom på, at de skal låse deres computer, så andre ikke får adgang til information, der ikke vedkommer dem.

TEMA 3

UNGÅ AT BIDE PÅ "PHISHING-KROGEN"

I skal lære målgruppen ikke at klikke på links i mails, som de ikke har tillid til.
En phishingmail er, hvor en hacker forsøger at franarre (fiske) éns personlige oplysninger som eksempelvis passwords. De prøver at lokke en til at klikke på et link i en mail, hvorefter de kan se de oplysninger, man indtaster. I skal derfor lære målgruppen at genkende phishingsmails, så de ikke ryger på krogen.



HVORDAN SKAL KOMMUNIKATIONS-KAMPAGNEN UDFORMES?

I bestemmer selv, hvordan kommunikationskampagnen skal udformes. Den kan se ud på mange måder, og I kan finde inspiration i listen her:

- **SoMe-kampagne**
- **Informationsmail**
- **Film (el. et storyboard til en film)**
- **Podcast**
- **Et event (lav evt. en drejebog for et event)**
- **Quiz**
- **Plakat**
- **Pjecer**

Overvej hvordan I kan lave budskabet sjovt, anderledes, kreativt og/eller nytænkende. Det er vigtigt, at kampagnen får målgruppen til at stoppe op en ekstra gang - og rent faktisk ændrer deres digitale adfærd. I kan med fordel tænke på situationer og scenarier, som målgruppen let kan relatere til.

Der forventes ikke et helt færdigudviklet produkt. Hvis I synes, I kommer bedst igennem med jeres budskab ved at lave et event, skal I ikke afholde et event, men I kan eksempelvis lave en drejebog for et event med et program, indholdspunkter m.m.

GODE RÅD TIL KAMPAGNEUDFORMING

Når I skal i gang med at lave selve kampagnen, er det en god idé at starte med at finde ud af, hvilket budskab I vil kommunikere, hvilken adfærd I ønsker at ændre og hvem I kommunikerer til. Her kan I med fordel undersøge lidt mere om emnerne og måske også få inspiration fra andre.

Derudover kan I få hjælp i diverse kommunikationsmodeller. Hvis ikke I allerede har arbejdet med nogen i undervisningen, kan I bruge de to modeller, som er beskrevet nedenfor. Det er 'Argumentationsanalysen' og 'Kommunikationsmodellen'.

Modellerne kan hjælpe jer i de valg, I træffer, når I udformer jeres kommunikationskampagne.

"MENNESKELIGE FEJL ER DEN HYPPIGSTE ÅRSAG TIL SIKKERHEDSBRUD. DERFOR ER UDDANNELSE I GOD IT-SIKKERHED MEGET VIGTIGT."

MODEL 1: ARGUMENTATIONSANALYSEN

I argumentationsanalyse skelner man mellem tre appelformer, der beskriver, hvordan man taler til modtageren på tre forskellige måder: Logos, etos og patos

Når man arbejder med budskaber, er det en god ide at overveje sin appelform.

I jeres præsentation skal I redegøre og argumentere for, hvordan I bruger de forskellige appelformer i jeres kommunikation. I kan sagtens anvende flere appelformer.

ETOS

Etos som appelform handler om at skabe troværdighed omkring afsenderen på baggrund af en person og hans eller hendes værdier. Hvis modtageren har tillid til afsenderen, er man oftest mere tilbøjelig til at give afsenderen ret i vedkommendes synspunkter og budskaber.

LOGOS

Denne appelform handler om at overbevise modtageren via en saglig og rationel argumentation. Man taler til modtagerens fornuft for at få dem til at indse rigtigheden af afsenderens synspunkter eller teorier. Logos bygger på fakta, tekstbelæg, statistikker og tal, altså dét som kan måles og dokumenteres.

PATOS

Denne appelform henvender sig til modtagerens følelser. Når afsenderen benytter patos som appelform, forsøger man at vække følelser som glæde, ophidselse, frygt, medlidenhed eller vrede hos modtageren for på den måde at overbevise ham eller hende om sit synspunkt.

MODEL 1

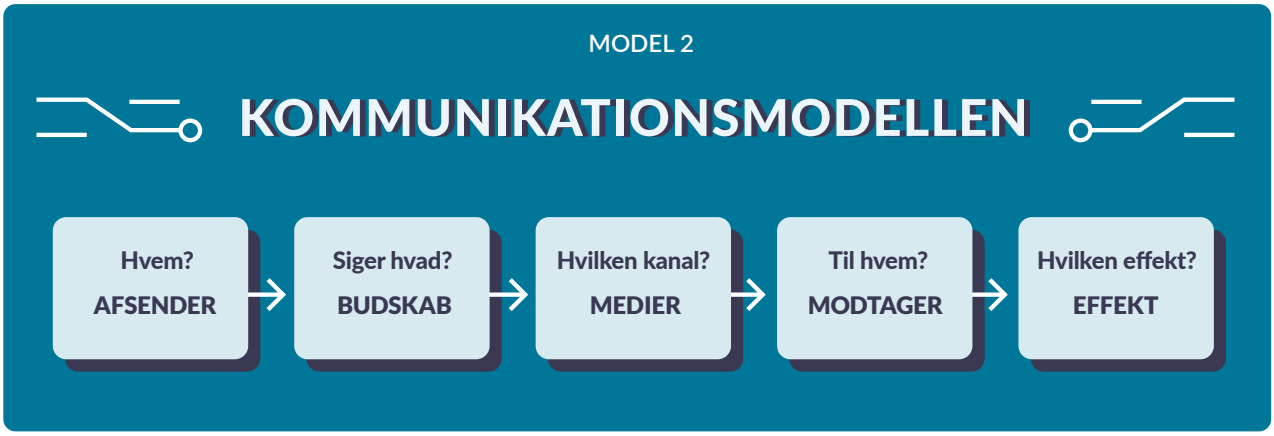
ETOS, LOGOS OG PATOS

TYPE	ETOS	LOGOS	PATOS
BETYDER	Når han/hun gør det, må det være godt	Tal, data, videnskabelige beviser Det logiske, det der tilsyneladende ikke kan sættes spørgsmålstegn ved	Gør det for min skyld Følelsestale
EKSEMPEL	"Fordi jeg siger det ..."	"Hvis du gør sådan sker der det og det ..." "70% af den danske befolkning ville gøre sådan..."	"Jeg bliver skuffet hvis du ikke gør det ..."

MODEL 2: KOMMUNIKATIONSMODELLEN

Kommunikationsmodellen, som I kan se herunder, består af fem faser, og kan hjælpe én, når man skal overveje sit budskab, udformning af budskabet, hvordan man vælger at kommunikere det samt om man via sine valg opnår den ønskede effekt.

I kan bruge kommunikationsmodellen til at beskrive jeres kampagne. I må gerne erstatte modellen med andre modeller, som I har kendskab til, og som I måske synes er bedre.



AFSENDER - HVEM?
"Hvem er det som siger noget?"
Afsender er den, der vil kommunikere et givent budskab.

BUDSKAB - SIGER HVAD?
"Hvad bliver der sagt?"
Afsenderens budskab er det, som han eller hun ønsker at kommunikere til modtageren.

MEDIE - I HVILKEN KANAL?
"Hvordan og hvor bliver det sagt?"
Medie er den kanal, der bruges til at formidle budskabet (det kan være alt fra en fysisk plakat, et nyhedsbrev, en kampagne på sociale medier osv.).

MODTAGER - TIL HVEM?
"Hvem bliver det sagt til?"
Modtageren er den person, afsenderen vil sende sit budskab til.

EFFEKT - MED HVILKEN EFFEKT?
"Hvad hører modtageren, der bliver sagt?"
Modtagerens afkodning af budskabet og en analyse af, hvordan modtager bliver påvirket af afsenderens meninger/budskab.

INSPIRATION

Inden I går i gang med at lave kommunikationskampagnen, kan I starte med at se disse tre videoer, som er lavet sammen med nogle super dygtige folk, der arbejder med kommunikation og it-sikkerhed til daglig. De vil hjælpe jer til at forstå missionen, og give jer nogle gode tips til stærke budskaber. Videoerne varer mellem 8-12 minutter:

VIDEO 1)
Tips og tricks til gode cyber awareness kampagner

VIDEO 2)
Når nørdede budskaber skal gøres spændende!

I finder videoerne under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/videomateriale2023/

JERES PRÆSENTATION

I skal forberede en præsentation af jeres kommunikationskampagne, hvor I redegør for missionen, fortæller om jeres proces med at finde frem til jeres løsning samt præsenterer selve løsningsforslaget.

I præsentationen skal I:

- Redegøre for jeres mission og den tematik, I har valgt at fokusere på
- Fortælle, hvordan I kom frem til jeres endelige løsningsforslag
- Præsentere jeres kommunikationskampagne (gerne med billeder, video m.m)
- Fortælle, hvordan I har anvendt analyseredskaber ex. argumentationsanalysen eller kommunikationsmodellen
- Argumentere for, hvilken effekt I tror, at jeres kampagne kan få hos jeres målgruppe.

Præsentationen skal have karakter af en kort præsentation, og må max tage 5 minutter.

DELTAG I EN NATIONAL KONKURRENCE

Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med. Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den til Styrelsen for It og Læring. Alle videoer vurderes af Cybermissionens dommerpanel.
Videoen skal uploades af den underviser, som har tilmeldt jer Cybermissionen. I finder link til uploadfunktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.

MISSION 3: FIND STØRRELSEN PÅ DINE DIGITALE FODAFTRYK

Vi hører ofte, at vores digitale handlinger på internettet afsætter spor, som andre kan registrere og fortolke. Mange af disse spor registreres passivt af søgemaskiner, sociale medier og lignende for at kunne bruges til målrettet markedsføring. Men de informationer, der registreres og gøres tilgængelige på internettet, kan også bruges aktivt, for eksempel i forbindelse med "**social engineering**" og "**spear phishing"**, hvor personlige informationer om offeret kan hjælpe med at målrette angrebet.

SOCIAL ENGINEERING

Social engineering er en metode, hvor en person manipulerer eller udnytter psykologiske og sociale faktorer for at få adgang til fortrolige oplysninger eller til at udføre uønskede handlinger. Det er en form for angreb, der fokuserer på at udnytte menneskelig adfærd i stedet for tekniske svagheder.

SPEAR PHISHING

Spear phishing er phishing, der er målrettet og personlig. I stedet for, at en phishing-e-mail sendes til mange mennesker, retter spear phishing sig mod specifikke enkeltpersoner eller organisationer. Angriberne bag spear phishing bruger ofte indsamlede oplysninger om deres mål, for eksempel navn, stilling, arbejdsgiver eller tidligere aktiviteter for at skabe en mere troværdig og målrettet phishing-kommunikation.

Mængden af direkte og indirekte personlige informationer, der er registreret om en person på internettet, kaldes ofte **personens digitale fodaftryk**; jo flere informationer, jo større fodaftryk.

JERES MISSION

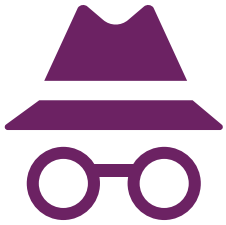
I denne mission skal I finde jeres digitale fodaftryk, dvs. de informationer, en angriber kan benytte til at fremstå imødekommende, have samme interesser eller på anden måde få offeret til at sænke sine parader overfor angriberens sociale manipulation.

Vi er alle forskellige og kan have meget forskellige digitale fodaftryk. Så i denne mission skal I finde jeres eget digitale fodaftryk, men I skal også sammenligne det med en jævnaldrende (for eksempel en af jeres venner) samt en meget ældre person, det kan for eksempel være et ældre medlem af jeres familie. Husk at spørge vennen og familiemedlemmet om lov først, da jeres interesse ellers kan virke som digital stalking.

Endelig skal I for hvert af de tre individer, I har undersøgt, identificere mindst én nøgleinformation, som I mener en angriber ville kunne benytte til at skabe en forbindelse og få jer selv, jeres ven og jeres familiemedlem til at sænke paraderne og være mere åbne overfor en henvendelse.

SOCIAL MANIPULATION

Vi har som mennesker en stærk trang til at høre til en gruppe, hvilket gør os modtagelige overfor henvendelser fra andre, der udnytter en fornemmelse af fællesskab, for eksempel tilhører samme gruppe eller befinder sig i en lignende situation. Sociale manipulatorer benytter ofte denne lighed til at skabe forbindelse til offeret og få dem til at tro på den baggrundshistorie, der benyttes til manipulationen. Eksempler kunne være, at angriberen har nogle sjældne sneakers til salg, leder efter nogen til at lufte sin hund, har gået på samme skole som offeret, er fan af offerets yndlingsband, der skal spille på Roskilde Festival, o.lign. Der er mange muligheder, men det gælder for angriberen om at finde noget, offeret er passioneret omkring, og som antyder fælles interesser og værdier, som kan danne en åbning til offeret.



SÅDAN KAN DINE INFORMATIONER BLIVE UDNYTTET

Når hackere bruger social manipulation til at indsamle informationer om enkeltpersoner, kan de have flere formål med disse oplysninger:

Identitetstyveri: Hackere kan bruge de indsamlede oplysninger til at stjæle en persons identitet. Dette kan være at bruge personlige oplysninger til at oprette falske konti, åbne kreditkort i offerets navn eller udføre andre økonomiske svindelnumre.

Økonomisk svindel: Ved at kende offerets personlige og finansielle oplysninger kan hackere udføre forskellige former for økonomisk svindel. Dette kan være at tømme bankkonti, foretage falske transaktioner eller begå bedrageri i offerets navn.

Adgang til systemer: Hackere kan bruge indsamlede oplysninger til at få adgang til beskyttede systemer eller netværk. Ved at kende brugernavne, adgangskoder eller andre autentificeringsoplysninger, kan de narre eller omgå sikkerhedsforanstaltninger og få ulovlig adgang til følsomme data eller ressourcer.

Phishing-angreb: Med personlige oplysninger i hånden kan hackere skræddersy phishing-angreb og forsøge at narre offeret til at afgive yderligere fortrolige oplysninger eller udføre skadelige handlinger. Dette kan omfatte at sende målrettede e-mails eller oprette falske websteder, der ligner legitime tjenester eller organisationer.

Det er vigtigt at være opmærksom på disse risici og være forsigtig med at dele oplysninger!

DIREKTE OG INDIREKTE INFORMATIONER

Nogle informationer fortæller direkte, hvad offeret er interesseret i, for eksempel hobbyer, kæledyr, yndlingsmusik samt billeder og videoer taget på ferie eller af bedste venner, der har det sjovt sammen i en eller anden aktivitet. Disse informationer findes ofte på sociale medier, i vlogs eller blogs, hvor offeret fortæller om sig selv og sine oplevelser. Disse informationer kan angriberen bruge direkte til at skabe den ønskede åbning. Andre informationer fortæller indirekte noget om offeret og skal derfor fortolkes, for at angriberen kan udlede de informationer, der skal bruges til angrebet. Det kan eksempelvis være, at angriberen finder et offentligt tilfængeligt referat fra en generalforsamling i den lokale golfklub, hvor det er beskrevet, hvem der blev valgt til bestyrelsen. Dermed kan det forventes, at offret er en passioneret golfspiller, ligesom bestyrelsesposter i skoler eller daginstitutioner fortæller, at offeret har mindre børn.

PRIVATE OG OFFENTLIGE INFORMATIONSKILDER

Som antydet ovenfor er der mange forskellige informationskilder, som kan fortælle om det påtænkte offers interesser.

Mange af disse informationskilder stammer fra private virksomheder eller enkeltpersoner, der opsamler og formidler informationer om individer. Disse informationer stammer ofte fra personen selv, enten direkte gennem sociale medier, blogs og vlogs, eller indirekte gennem profilering af deres adfærd, for eksempel deres lokationsdata, søgehistorik eller cookies.

Andre informationskilder er offentlige systemer, der registrerer forskellige informationer om borgerne, som herefter offentliggøres. Dette kan eksempelvis være telefonbøger (for eksempel krak.dk), som kan vise

15

offerets adresse, tingbogen, der indeholder informationer om ejerskab og værdi af ejendomme, som fortæller noget om offerets indtægt (hvis ejendomsværdien er høj), kommunens weblager, som fortæller om bolig og byggesager, eller virksomhedsregistre (virk.dk eller proff.dk), som kan fortælle noget om virksomheder, som offeret kan eje eller lede. Der er mange andre typer offentlige registre, som offentliggør informationer, der kan bruges til at danne sig et billede af det påtænkte offer for social manipulation. Det drejer sig bare om at finde dem gennem forespørgsler til forskellige søgemaskiner.

Mange af de informationer, man kan finde gennem private informationskilder, kan offeret minimere gennem privatlivsfremmende teknologier eller ved simpelthen ikke at have profiler på sociale medier. De offentlige informationskilder drives ofte af myndigheder, som stiller informationer til rådighed, der ved lov skal være offentlige tilgængelige, så disse informationer er umulige for det påtænkte offer at holde hemmelige. Som privatperson er det derfor nyttigt at vide, hvilke typer af informationer myndighederne offentliggør om ens person og ejendomsforhold. Med den viden, kan man som borger bedre gennemskue om en, der udgiver sig for fra at være fra en offentlig myndighed, faktisk også er det, eller om vedkommende bare udnytter offentlig tilgængelige informationer.

JERES MISSION

Denne mission består af tre trin, som dokumenteres med en præsentation.

1

Find størrelsen af jeres digitale fodaftryk. Start med at se på, hvilke digitale informationer I selv lægger på nettet gennem sociale medier eller andre private informationskilder. Prøv så at se, om I kan finde jer selv i andre private informationskilder, for eksempel om I er tagget i billeder på Instagram, i videoer på TikTok eller blandt jeres "venner" på Facebook. I kan også kigge på likes på billeder og videoer, I har lavet. Endelig skal I undersøge, hvilke informationer I kan finde i offentlige informationskilder, ekesempelvis via en søgemaskine, på Aula eller jeres skoles hjemmeside, jeres fritidsaktivitet. Husk på, at Aula kræver login, så angriberen har måske ikke adgang til mange af disse informationer, mens skolens hjemmeside normalt er offentligt tilgængelig. Sammenlign jeres undersøgelser i gruppen og diskuter, hvad I er kommet frem til.

2

Der er typisk ikke mange informationer fra offentlige informationskilder i jeres aldersgruppe, men prøv at gennemføre de samme tre trin med et ældre medlem af jeres familie. Husk at spørge om lov først, da det ellers vil være at betragte som stalking.

3

Nu skal I analysere de informationer I har fundet om jer selv. Hvilke direkte informationer kan en angriber bruge til at udlede jeres præferencer? Hvad fortæller jeres online tilstedeværelse om jer selv og jeres liv? Og hvordan kan en angriber udnytte det til at blive fortrolig med jer og få jer til at sænke jeres parader? Er der også nogle indirekte informationer, for eksempel billeder fra en ferie, en koncert eller en festival, hvor en angriber kan komme tættere på ved at lade, som lade som om de har været til samme begivenhed? Det kan også være informationer om jeres præferencer gennem farven af jeres tøj (yndlingsfarve), plakater med musikere, sportsidoler eller lignende på billeder fra jeres værelser, osv.

4

Overvej, hvordan I ville bruge disse informationer til at indsmigre jer på jer selv. Skriv en dialog med jer selv, hvor I viser, hvordan angriberen benytter informationer fundet i jeres digitale fodaftryk og får jer til at sænke paraderne. Opfør evt. denne dialog som et rollespil, og lad det være en del af jeres præsentation.

JERES PRÆSENTATION

I skal forberede en præsentation af jeres undersøgelse, hvor I redegør for missionen, fortæller om jeres proces

med at finde frem til informationen om jer selv, samt præsenterer den information, I har fundet, og hvilke tanker I gør jer om det.

I præsentationen skal I:

- Redegøre for jeres mission og hvordan I har grebet opgaven an.
- Fortælle, hvilke typer af information I har fundet i jeres research, hvad der overraskede jer mest, og hvor I efterfølgende har gjort noget for at gøre information om jer selv mere privat.
- Analysere hvordan en evt. angriber vil kunne bruge den information, I har fundet, imod jer. Lav evt. en skærmoptagelse af den dialog, I har lavet, eller fremfør dialogen.
- Fortælle hvis I har anvendt nogle særlige metoder eller analyseredskaber etc.
- Præsentationen må max tage 5 minutter.

DELTAG I EN NATIONAL KONKURRENCE

Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med.

Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den til Styrelsen for It og Læring. Alle videoer vurderes af Cybermissionens dommerpanel. Videoen skal uploades af den underviser, som har tilmeldt jer Cybermissionen. I finder link til uploadfunktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.

MISSION 4: HAD ONLINE OG DESINFORMATION

Hate speech eller hadefulde ytringer på dansk, er et fænomen, som vi skal være opmærksomme på, og ikke mindst forstå mekanismerne bag.

Når hadefulde ytringer bliver spredt, kan det føre til diskrimination, stigmatisering, forfølgelse og voldelige handlinger mod den gruppe eller de personer, som er mål for disse ytringer. Hate speech kan føre til, at man føler sig truet eller give en følelse af usikkerhed og frygt. Det, der rettes mod en, kan opleves meget voldsomt. Det kan føre til, at man føler sig ekskluderet fra samfundet.

Hate speech kan være med til at skabe en negativ samfundskultur, hvor intolerance og had pludselig bliver normaliseret, og hvor forskellige grupper bliver modarbejdet i stedet for at blive inkluderet.

Sker det, er vi ved at underminere fundamentet for et demokratisk samfund, hvor ytringsfrihed og respekt for menneskerettighederne er centrale værdier - og det vil være meget alvorligt. Derfor er det vigtigt, at vi sammen bekæmper hate speech og fremmer en inkluderende og respektfuld dialog, hvor forskellige synspunkter kan udtrykkes uden at såre eller diskriminere andre.

JERES MISSION

I jeres gruppe skal I udvikle en kommunikationskampagne, som kan bidrage til at mindske hate speech. Kampagnen skal henvende sig til unge på jeres egen alder. Nedenfor finder I en masse baggrundsinformation om blandt andet hate speech og filterbobler, to cases, hvoraf I skal vælge én, som kan være omdrejningspunkt for jeres kampagne. Når I har lavet kampagnen, skal I også forberede en kort præsentation, hvor I fortæller om jeres tanker bag.

HAD KOMMER I MANGE FORMER - MEN HVORDAN DEFINERER VI DET?

Selve definitionen af hvad der er hate speech, og hvad der bare er dårlig opførsel, er nogle gange sløret og afhængig af konteksten.

FN har beskrevet hadefulde ytringer på følgende måde:

"Enhver form for kommunikation i tale, skrift eller adfærd, der angriber eller bruger nedsættende eller diskriminerende sprog med henvisning til en person eller en gruppe på grundlag af, hvem de er, med andre ord baseret på deres religion, etnicitet, nationalitet, race, farve, afstamning, køn eller andre identitetsfaktorer."

FNs definition af hate speech i tekstboksen udelader dog nogle vigtige grupper, der møder online had. En anden og bredere definition lyder:

"Sprog, der bruges til at udtrykke had mod en målgruppe eller er beregnet til at være nedsættende, ydmygende eller fornærme medlemmer af gruppen."
(Davidson, 2017).

Den anden definition er afgørende, da hadefulde ytringer dækker bredt. I vores moderne, politiske miljø kan selv politiske partier ty til hadefulde ytringer mod et andet parti og dets tilhængere, hvis deres værdier ikke stemmer overens.

Med definitionen af hadefulde ytringer på plads kan det nu diskuteres: Hvorfor er det så vigtigt? Når der er en stigning i hadefulde ytringer, kan det have en lang række kritiske konsekvenser i hele samfundet. Et eksempel er, at når der foregår hadefulde ytringer online, kan det føre til mere direkte handlinger - også uden for internettet. Når en gruppe mennesker eksempelvis bliver dæmoniseret online, kan nogle individer føle, at det er mere moralsk okay at udøve fysisk vold mod denne gruppe.

HATE SPEECH I POLITIK

Når politikere bruger hadefulde udtalelser, kan det have alvorlige konsekvenser for samfundet som helhed. Det kan føre til øget polarisering, diskrimination, stigmatisering og endda vold. Samtidig kan det underminere de grundlæggende værdier i et demokratisk samfund, herunder ytringsfrihed, lighed og respekt for menneskerettighederne.

Hate speech i politik kan også bidrage til at normalisere ekstreme holdninger og adfærd i samfundet, og det kan føre til en kultur, hvor hadefulde ytringer og handlinger bliver mere acceptable.

Derfor er det vigtigt at bekæmpe hate speech i politik og fremme en inkluderende og respektfuld dialog, der er baseret på fakta og med respekt for forskelligheder.

HATE SPEECH PÅ SOCIALE MEDIER

Hate speech er desværre blevet udbredt på rigtig mange sociale medier af flere årsager.

3 af de primære årsager er:

1. Sociale medier giver mulighed for at nå ud til et stort publikum på kort tid, og det kan være fristende for nogle at bruge det som et middel til at sprede hadefulde ytringer og holdninger.

2. Anonymiteten på sociale medier kan give en følelse af immunitet, som kan føre til, at nogen udtrykker sig mere aggressivt og hensynsløst, end de ville gøre i virkeligheden.

3. Algoritmer og indholdsforslag på sociale medier kan gøre, at folk kommer i kontakt med mere ekstreme og polariserede synspunkter. Dette kan skabe en "ekkokammer-effekt" også kaldet filterbobler, hvor brugere kun ser og hører synspunkter, der bekræfter deres egne holdninger. Det kan forstærke eksisterende fordomme og stereotyper.

Alt i alt er der flere faktorer, der bidrager til udbredelsen af hate speech på sociale medier, og det er vigtigt at forstå disse for at kunne bekæmpe problemet effektivt.

HVORDAN HÆNGER DET SAMMEN MED CYBERSIKKERHED?

Hate speech er ofte en forløber for mere ekstreme handlinger, og kan tiltrække opmærksomhed fra hackere og cyberkriminelle, der ønsker at udnytte situationen.

For eksempel kan en gruppe, der udtrykker hadefulde synspunkter mod en bestemt befolkningsgruppe, blive mål for et cyberangreb fra en anden gruppe, der er uenig i deres synspunkter. Dette kan føre til hacking af deres hjemmesider eller konti på sociale medier, eller til spredning af skadeligt malware.

Desuden kan hate speech føre til en øget risiko for cyberstalking og online chikane, som kan have alvorlige konsekvenser for den person, der er mål for disse angreb. Det kan inkludere krænkelser af personlige oplysninger, identitetstyveri og endda trusler mod personens fysiske sikkerhed.

Derfor er det vigtigt at bekæmpe hate speech for at beskytte cybersikkerheden og sikre, at online-platforme og netværk forbliver sikre og pålidelige for alle brugere. Det kan kræve en kombination af teknologiske og sociale løsninger, herunder styrket online-overvågning, forbedret uddannelse om cybersikkerhed og fremme af respektfuld adfærd og tolerance i online fællesskaber.

JERES MISSION

I skal nu på en mission omkring hate speech.

DELMISSION 1: TO CASES

I skal vælge en af de to cases nedenfor og diskutere de tilhørende arbejdsspørgsmål.

CASE 1:

TROLDEFABRIKKER PÅVIRKER DEMOKRATISKE VALG

En troldefabrik er en organisation, som er ansvarlig for at skabe og sprede desinformation og propaganda på internettet med henblik på at påvirke offentlige meninger og politiske beslutninger. De består ofte af et team af professionelle skribenter, programmører og eksperter i sociale medier, der arbejder sammen for at producere og sprede falske nyheder, desinformation og manipulation på sociale medieplatforme som Facebook, Twitter, Instagram og andre. Disse fabrikker er blevet kraftigt kritiseret for at påvirke offentlige valg og politiske beslutninger i forskellige lande.

CASE 2:

HØJRERADIKALE ONLINE-GRUPPER

Mennesker der bliver hængt omringet af kutteklædte Ku Klux Klan-medlemmer, terrorangreb på muslimer, Hitler der heiler, hagekors der vælter frem i et væk. Alt dette er klip, som vises på en Discord-kanal for helt unge mennesker. Gruppen er skabt for, at de sammen kan dele og tale om ekstremt voldeligt og racefjendsk indhold. I Danmark er der flere og flere tilfælde af mindreårige, som er havnet i højreradikale online-grupper med risiko for at blive hjernevaskede og voldsparate ude i den virkelige verden, og hvor det, som bliver formidlet i disse grupper, simpelthen er faktuelt forkert.

*Lyt evt. til podcasten "Hitler på teenageværelset" produceret af DR (Genstart) d. 22. marts 2023

ARBEJDSSPØRGSMÅL:

- Hvordan er hate speech på spil i jeres valgte case?
- Hvilken indflydelse har sociale medier og teorien om filterbobler i den givne case?
- Hvordan kan det, der udfolder sig i casen, være en trussel for det danske demokrati?
- Diskuter, om denne form for hate speech kan motivere til cyberangreb? Og hvem er det, det kan motivere?

DELMISSION 2: LAV EN OPLYSNINGSKAMPAGNE

For at bekæmpe hate speech er det vigtigt, at vi får gjort unge opmærksomme på problemet ved det, samt hvorfor de skal være varsomme overfor den information, de møder.

I skal derfor lave en oplysningskampagne til unge om den problemstilling. I skal tænke over form, budskab og fremføring. På baggrund af jeres arbejde med delmission 1 kan I overveje, hvad det er vigtigst, at I får kommunikeret, så den unge målgruppe forstår alvoren af hate speech.

HVORDAN SKAL KOMMUNIKATIONSKAMPAGNEN UDFORMES?

I bestemmer selv, hvordan kommunikationskampagnen skal udformes. Den kan se ud på mange måder, og I kan finde inspiration i listen her:

- Kampagne til sociale medier
- Film (eller et storyboard til en film)
- Podcast
- Et event (lav evt. en drejebog for et event)
- Quiz
- Plakat
- Pjece
- Animationsfilm

Overvej, hvordan I kan lave budskabet sjovt, anderledes, kreativt og/eller nytænkende. Det er vigtigt, at kampagnen får målgruppen til at stoppe op en ekstra gang - og rent faktisk ændrer deres digitale adfærd. I kan med fordel tænke på situationer og scenarier, som målgruppen let kan relatere til.

Der forventes ikke et helt færdigudviklet produkt. Hvis I synes, I får jeres budskab bedst frem ved at lave et event, skal I ikke nødvendigvis afholde et event. Men I kan eksempelvis lave en drejebog for et event med et program, indholdspunkter m.m.

JERES PRÆSENTATION

I skal forberede en præsentation af jeres kommunikationskampagne, hvor I redegør for missionen, fortæller om jeres proces med at finde frem til jeres løsning og præsenterer selve kampagnen.

I præsentationen skal I:

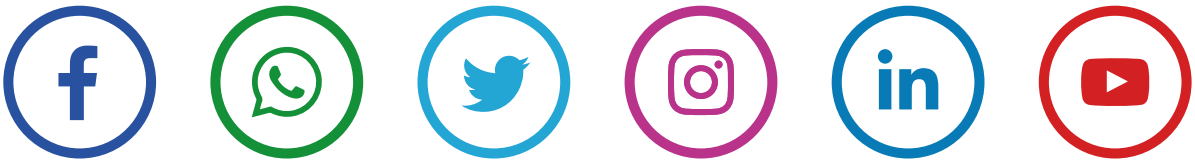
- Redegøre for jeres mission og den case, I har valgt at fokusere på.
- Fortælle hvordan I kom frem til jeres endelige løsningsforslag.
- Præsentere jeres kommunikationskampagne (gerne med billeder, video, skærmoptagelse, animation mm.) .
- Fortælle hvis I har anvendt nogle særlige metoder eller analyseredskaber etc.
- Argumentere for, hvilken effekt I tror, jeres kampagne kan få hos jeres målgruppe.

Præsentationen må max tage 5 minutter.

DELTAG I EN NATIONAL KONKURRENCE

Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med. Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den til Styrelsen for It og Læring. Alle videoer vurderes af Cybermissionens dommerpanel. Videoen skal uploades af den underviser, som har tilmeldt jer Cybermissionen. I finder link til uploadfunktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.

MISSION 5: DEL OG HERSK! STYR DINE DATA!



De sociale medier er en integreret del af vore daglige liv. Det er her, vi kommunikerer, deler nyheder, vedligeholder kontakter med folk, vi ikke ser så tit, og finder nye bekendtskaber. At interagere med sociale medier er en essentiel del af vores sociale dannelse og relationer.

Den sociale interaktion betyder, at vi deler mange forskellige typer af data med hinanden fra billeder til tekst, videomateriale, links, lyd og meget mere. Desværre kan det materiale bruges af cyberkriminelle til at sammenstykke et billede af os og til at finde en sårbarhed, hvor de kan angribe. Angreb kan være alt fra, at vi trykker på et link for en konkurrence for et produkt, vi gerne til vinde, til at vi modtager personlige henvendelser på chat eller mail, der fortæller os, at vi skal gøre noget. Vores profiler på sociale medier kan også blive hacket og overtaget af andre, hvilket ikke er særlig sjovt.

Den sociale interaktion er dermed god for os, men desværre også god for cyberkriminelle. Det gælder om at finde en god balance, hvor vi stadig kan være sociale online, men samtidig ikke serverer alting til de cyberkriminelle.

PERSONDATAFORORDNINGEN

I EU besluttede man i 2018, at Persondataforordningen (GDPR) skulle gælde for alle de online services, vi modtager og bruger i EU. Generelt går den ud på at stille krav til virksomhederne og deres brug af de data, vi giver dem. De skal tænke på, hvordan de opbevarer data, hvad de gør med dem og hvem de deler dem med. Samtidig har vi som brugere af de services bl.a. ret til at sige nej til, at de må dele data med andre.

Ifølge Persondataforordningen skal virksomheder udarbejde en analyse af deres egen brug af data, beskrive processerne i og udenfor virksomheden, som modtager og modificerer data og beskrive, hvor der er størst risiko for, at der sker noget med data. Ligeledes skal de overveje, hvad de kan gøre ved sårbarheder i virksomhedens databehandling. Nogle data er vigtigere at se på end andre, og derfor skal virksomhederne også kategorisere de data, de bruger.

DATATYPER

Man skelner i Persondataforordningen mellem data, der er identificerbare og dem, der ikke er det. Identificerbare betyder data, hvorfra man umiddelbart kan identificere en person (altså vide, at det er præcist dig eller din ven, som data tilhører). Eksempler på identificerbare data er personnummer, adresse, betalingsoplysninger m.m. I persondataforordningen taler man om almindelige personoplysninger såsom navn, adresse, telefonnummer osv. og følsomme personoplysninger såsom helbredsoplysninger, biometriske data, religion m.m. Det er klart, at man som virksomhed skal passe godt på alle typer af data, men at de følsomme personoplysninger skal have mere sikkerhed.

JERES MISSION

I denne mission skal I arbejde med eksempler på data, som deles på sociale medier samt nogle af de cybersikkerhedsangreb, der kan sættes ind og anvendes mod os. I skal arbejde med forskellige opgaver, der viser sårbarheder ved ukritisk anvendelse af data på sociale medier. I Missionen skal I finde løsninger på, hvordan man kan forhindre sårbarheder, så man fortsat kan få stillet sit behov for at være social online.

Som en del af missionen skal I løse en række forskellige opgaver på en læringsplatform, der hedder Haaukins. Her får I mulighed for at arbejde med "etiske cybersikkerhedsangreb". Haaukins er en virtuel platform med et sikkert miljø. Derfor kan man der se, hvad cyberkriminelle kan finde på uden at blive angrebet i det virkelige liv. På Haaukins er der et område med opgaver (chal-

lenges), der alle er knyttet til brug af kendte sociale medier. Missionen er knyttet til Peacock, som ligner et kendt socialt medie. Missionen har et teknisk element, men ser dog mest på data og databeskyttelse. Ved løsning af opgaverne på Haaukins/Peacock kommer man ud for at skulle bruge forskellige tekniske redskaber for at lede efter information, som også cyberkriminelle ville lede efter.

Som afslutning på missionen skal I udarbejde en præsentation, der belyser nogle af de problemstillinger, man som ung har med cybersikkerhed på de sociale medier. I skal også diskutere de dilemmaer, der kan ligge i at dele forskellige typer data samt beskrive løsninger, der kan sikre, at unge kan være online uden at være for nervøse for cyberangreb eller misbrug på anden vis.

TRIN 0: REGISTRERING I HAAUKINS/PEACOCK

For at kunne arbejde med Haaukins/Peacock, skal I have et link af jeres underviser. Når I klikker på dette link, skal I registrere jer individuelt på platformen ved at trykke på "Sign Up" oppe i højre hjørne. Gå derefter til oversigten over "challenges" og vælg opgaven i kategorien "Starters" ved navn "Sanity check-static". Når I har læst indholdet i opgaven, skal I trykke på "Connect" oppe i højre hjørne for at tilgå jeres virtuelle lab. I det virtuelle lab skal I åbne Firefox og gå til siden "sanity-checks.hkn". Kopiér flaget og sæt det ind i "submit feltet" på challenge-siden i jeres egen browser. Så er I klar til at starte på de egentlige opgaver i trin 1-3.

TRIN 1: LOG PÅ HAAUKINS/PEACOCK OG LAV (MINDST) 5 OPGAVER

På trin 1 arbejder I med 5 forskellige challenges, der alle er knyttet til det at dele forskellige typer af data med hinanden på sociale medier. De 5 challenges er:

1. **Anonymous sandworms part 1**
   Den første challenge omhandler de oplysninger, vi deler med hinanden igennem de interaktioner, vi har på sociale medier eller lignende.
   Reflekter over, hvad I selv deler og tænk over, om det kan give problemer af den art.
2. **Anonymous sandworms part 2**
   Det er ikke altid gennem tekst, at vi deler oplysninger. Denne challenge omhandler de billeder, vi deler, og de oplysninger, som optræder visuelt på dem. Derfor er det vigtigt at være bevidst om de informationer, som vi deler igennem de billeder, vi lægger på sociale medier eller lignende. For eksempel visuel information, der kan bruges til at finde ud af, hvor vi er.
   Hvor meget deler I billeder og trykker på andres billeder? Reflekter over, hvordan man kan sikre sig bedre.
3. **Anonymous sandworms part 3**
   I denne challenge har vi igen fokus på de data vi deler, når vi interagerer med hinanden på sociale medier eller lignende. Denne challenge bygger på det, vi har lært i de 2 første challenges. Denne gang skal vi i stedet for relationer prøve at misbruge de informationer, som vi indsamler, til at få adgang til en anden brugers profil på Peacock.hkn/.
   Hvad læres der her? Er det noget, I har været ude for selv? Hvordan skal man forholde sig til sådan et "angreb"?
4. **The Cultural Code**
   En "mister important" på Peacock.hkn skal til et kulturevent. Men billetterne kan være falske. Se på Peacock.hkn og undersøg sagen.
5. **The Golden Seagull**
   I denne challenge er der fokus på at forstå, hvilke informationer der er indlejret i de billeder, vi deler.
   Nå I har løst disse challenges, skal I gå videre til Trin 2.

TRIN 2: LAV EN SÅRBARHEDSANALYSE AF JERES BRUG AF FORSKELLIGE TYPER AF DATA PÅ SOCIALE MEDIER

Persondataforordningen er kun for virksomheder. Men det kan være interessant at undersøge, hvordan en sårbarhedsanalyse vil se ud for den måde, vi bruger sociale medier på, og hvordan delingen af forskellige typer af data ser ud.

Derfor skal I, i dette trin, udarbejde en oversigt over de typer af data, I typisk deler med jeres venner og familie. Lav enten en analyse hver især, eller udvælg én i gruppen, som I laver analysen på. Identificer om de oplysninger, I finder frem til, er sårbare data eller ej, og om man kan identificere jer direkte fra dataene eller ej.

Lav en sårbarhedsanalyse over data, deling og hvad I gør med data på sociale medier. Brug gerne den indsigt, I har opnået i Trin 1, i analysen. Diskuter derefter, jeres fund og hvad de kan betyde for jeres anbefaling af, hvad man skal gøre for at beskytte sig lidt bedre, men alligevel være social online.

SÅRBARHEDSANALYSE

Sårbarhedsanalyser kan udføres på forskellig vis. Som en del af Persondataforordningen ser virksomheder på, hvilke typer af data de bruger og sender til andre, hvad der kan ske med dem og hvad sandsynligheden er for, at der sker noget, der ikke bør ske. Den analyse danner grundlag for en diskussion af, hvor der er størst risiko for, at data kommer i andres hænder (sårbarheden er størst). Den indsigt kan bruges til at arbejde med forskellige løsninger, der kan mindske risikoen.

Udarbejd et skema over forskellige typer af data, I deler på sociale medier. Skemaet kan se ud som herunder:

SKEMA

DATA OG DATATYPE	PROCES (beskriv hvad der sker med data)	HVAD KAN DER SKE (giv eksempel på, hvad der kan ske)	RISIKO FOR AT DER SKER NOGET I PROCESSEN (vurder gerne sandsynligheden for, at det sker, og forklar, hvordan I er kommet frem til det)	HVAD SKAL DER TIL, FOR AT UNDGÅ AT DET SKER (eller at det sker mere sjældent)

BAGGRUND FOR TRIN 1-2

For at kunne arbejde med missionen skal I vide noget om Haaukins/Peacock.

HAAUKINS/PEACOCK

Haaukins er en virtuel læringsplatform, hvor alle med interesse i cybersikkerhed kan træne og lære mere om emnet i et sikkert miljø. Filosofien bag platformen er, at man skal lære at tænke som en hacker for at forstå, hvad og hvordan man skal gøre for at komme de cyberkriminelle i forkøbet. I Haaukins skal man finde såkaldte flag. Flagene er visualiseret som en kode og ser sådan ud: "HKN{et_eller_andet_text}". Flagene kan findes i tekst i koden på skærmen. Når man har fundet flaget, kopieres flaget til "challengesiden" og flaget indsættes. Dermed bliver en challenge løst.

Peacock er det sociale netværk på Haaukins. Her vil I kunne agere nogenlunde, som I plejer på et socialt medie. Dog vil I simulere at være en cyberkriminel, som skal forsøge at finde data om de forskellige personer på Peacock ud fra de data, de har delt om hinanden. Men I vil ikke kunne bruge det sociale netværk som I plejer ved at oprette jer som brugere, sende billeder til venner og finde andre venner der. I kan kun anvende PEACOCK til at løse den opgave, I får stillet.

HAAUKINS/PEACOCK findes på https://www.peacock/. I skal spørge jeres underviser, hvordan I finder dertil og finder opgaverne.

JERES PRÆSENTATION

For at gennemføre missionen, skal I forberede en præsentation.

I præsentationen skal I:

- Redegøre for jeres mission.
- Reflektere over, hvilke typiske problemer og dilemmaer man som ung kan komme havne i i forhold til cybersikkerhed på sociale medier.
- Præsentere jeres forslag til, hvordan I ville forhindre cyberkriminelle I at bruge jeres data på sociale medier.

Præsentationen skal være kort, og må max tage 5 minutter.

DELTAG I EN NATIONAL KONKURRENCE

Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med. Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den til Styrelsen for It og Læring. Alle videoer vurderes af Cybermissionens dommerpanel. Videoen skal uploades af den underviser, som har tilmeldt jer Cybermissionen. I finder link til uploadfunktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere

LÆRERVEJLEDNING TIL PEACOCK

TIL UNDERVISEREN, SOM ØNSKER AT ARBEJDE MED MISSION 5

Baggrund

I denne cybermission, skal eleverne arbejde i et virtuelt cybertræningsmiljø, som hedder Haaukins. Her kan eleverne tilgå hjemmesider, sociale netværk mm. I et lukket virtuelt miljø. Herunder bla. Peacock, som er omdrejningspunktet i denne mission. Så længe eleverne bliver i Haaukinsmiljøet og anvender den browser, der er i det virtuelle miljø, sker der ikke noget, og eleverne kan udføre og udforske etisk hacking, social engineering og phishing uden at være nervøse for at overtræde lovgivningen.

For at få adgang til Haaukins, skal du skrive en mail til Kristian Kjær Helmer Larsen på khkl@es.aau.dk.

Denne mail skal indeholde:

- Skolens navn
- Hvornår skal I have adgang fra (dato og tidspunkt)
- Hvor længe I skal have adgang (slutdato)
- Hvor mange elever, skal have adgang?

Kristian vil herefter sende dig et link som eleverne skal oprette sig som brugere på.
Hvis I oplever problemer med challenges eller Haaukins, kan I til hver tid kontakte Kristian.

Find alle løsningerne

Du finder alle løsningerne på de challenges eleverne skal igennem i den følgende lærervejledning.

Såfremt I får behov for det, kan eleverne finde en oversigt over Linux-kommandoer, på denne hjemmeside: https://cheatography.com/davechild/cheat-sheets/

HAAUKINS
VIRTUALIZED CYBER SECURITY TRAINING

LÆRERVEJLEDNING TIL PEACOCK (Mission 5)

Kristian Kjær Helmer Larsen 17/03/2023

Peacock er en platform, som efterligner et populært socialt medie. Peacock-opgaverne er et sæt af opgaver, som forholder sig til vores privatliv på sociale medier. Idéen med opgaverne er at introducere eleverne til privatlivskonceptet på sociale medier uden at gå for meget i dybden med den tekniske side af hacking-disciplinen.

idéen med opgaverne er at introducere eleverne til privatlivskonceptet på sociale medier uden at gå for meget i dybden med den tekniske side af hacking-disciplinen.
Opgaverne ligger hovedsageligt indenfor kategorien **OSINT** (open-source intelligente), som handler om at samle informationer, som ligger offentligt tilgængelige. Det bliver simuleret i Peacock, og opgaverne illustrerer problematikker, som er gode at kende, når man interagerer med hinanden digitalt.

LÆRINGSMÅL

- Kompetencer til at begå sig sikkert på sociale medier.
- Kendskab til typer af data, som vi deler sammen med vores billeder.
- Basale færdigheder inden for cybersikkerhed.
- Kompetencer til at navigere Haaukins på egen hånd.

OPGAVER OG LØSNINGER

Opgaverne, som er inkluderet i denne cybermission, vil herefter blive refereret til som challenges. Der er i alt 11 challenges. Rækkefølgen, de er beskrevet i herunder, vil også være den anbefalede, når eleverne skal løse opgaverne. Det er en god idé at lægge små pauser ind undervejs og også at gennemgå nogle af opgaverne løbende, så elever ikke sidder fast i en opgave i længere tid. De første 5 challenges er tænkt som de vigtigste for at nå læringsmålene beskrevet herover. Platformens sprog er engelsk og derfor vil der være en del engelske betegnelser i det følgende, så det matcher beskrivelserne i Haaukins.

De første 5 challenges er:

1. Anonymous sandworms part 1
2. Anonymous sandworms part 2
3. Anonymous sandworms part 3
4. The cultural code
5. The Golden Seagull

EKSTRA OPGAVER

Opgaver som kan gives til de hurtige elever, som har brug for ekstra udfordringer, når de første 5 er løst.

6. The yellow snitch
7. Johns weird comment!?
8. The hash hack:
9. Rockies code
10. The Graduation Party
11. The Suitcase

ANONYMOUS SANDWORMS PART 1:

Den første challenge omhandler de oplysninger, vi deler med hinanden igennem interaktioner på sociale medier eller lignende. Essensen i denne opgave er at forstå, at selvom vi ikke deler bestemte oplysninger direkte, fortæller den måde, vi interagerer med hinanden på, meget om, hvem vi er og vores relationer til andre, f.eks. vores familierelationer.

Challenge-beskrivelse på Haaukins

We suspect that the recent robbery on Wetcompany has been done by the group of criminals called ”Anonymous sandworms”. So far investigations shows that they might use peacock.hkn as a platform to communicate. We need you to find the real identity of criminal Mister Beef.

Flag form: HKN{Firstname_FathersFirstname_BrothersFirstname}

Løsning:

1. Gå til peacock.hkn/ i firefox på den virtuelle kali-maskine inde på Haaukins.
2. Dan dig et overblik over de forskellige posts og brugere på platformen ved at scrolle lidt rundt og måske klikke ind på din egen og andre profiler.

3. Vi skal finde fornavnet på Mister Beef, og navnene på hans bror og far. Dette kan gøres ved at læse kommentarsporene på forskellige posts.
4. Faren og brorens brugernavne har det samme efternavn.
5. Ud fra ovenstående kommer man frem til følgende flag HKN{Miguel_John_Benjamin} (læg mærke til, at hvert navn er med stort forbogstav ligesom i flag format).

ANONYMOUS SANDWORMS PART 2

Det er ikke altid gennem tekst, at vi deler oplysninger. Denne opgave omhandler de billeder, vi deler, og de oplysninger, som optræder visuelt på dem. Det er vigtigt at være bevidst om de informationer, som vi deler igennem de billeder, som vi deler på sociale medier eller lign. For eksempel visuelle informationer, der kan bruges til at finde ud af, hvor vi er.

Challenge-beskrivelse på Haaukins

Good job identifying this fella! Unfortunately, he doesn't have an address in our system! Please help us find out where he is living at the moment. We need to catch him before the next robbery! Go to peacock.hkn and find out.

Flag format: HKN{city_streetname} Ex `HKN{greve_strand_grevehaven}`

Løsning:

1. Gå til peacock.hkn/
2. Find Ginas post med et hotel.
3. Der er et navn på hotellet på billedet.
4. Indtast navnet på hotellet på google, og du vil få adressen i dine søgeresultater
5. Flaget er HKN{vesterø_havn_havnebakken}

ANONYMOUS SANDWORMS PART 3

I denne challenge har vi endnu engang fokus på de data, vi deler, når vi interagerer med hinanden på sociale medier eller lignende. Denne challenge bygger på det, vi har lært i de 2 første challenges. Denne gang skal vi i stedet for relationer prøve at misbruge de informationer, som vi indsamler, til at få adgang en anden brugers profil på peacock.hkn/.

Challenge-beskrivelse på Haaukins

Great job on profiling the criminal Mister Beef! New intel tells us that he might use his girlfriend's account to communicate with the other members of Anonymous sandworms.

Go to peacock.hkn and obtain access to her account so we can find out.

Løsning:

1. Gå til peacock.hkn
2. Find en post fra Febrina, hvor hun poster om sin rejseblog. Der har Gina skrevet sin e-mailadresse.
3. Gå til peacock.hkn
4. Find nu hendes kælenavn, som kan findes i hendes egne nye posts
5. Prøv nu at logge ind på hendes profil ved at bruge e-mailadressen: ginababe@hmail.hkn og password: nina!

THE GOLDEN SEAGULL

I denne challenge er der fokus på at forstå, hvilke informationer der er indlejret i de billeder, vi deler. For at løse opgaven skal eleverne søge efter information om, hvad exif data er.

Challenge-beskrivelse på Haaukins

Someone from Anonymous sandworms has stolen the very valuable painting "The Golden Seagull". Please go to peacock.hkn and help us locate the painting. The culprit might "exif" it in a one of a kind restaurant. Flag form: HKN{country_streetname} Ex `HKN{denmark_fugle_rd}`

Løsning:

1. Gå til peacock.hkn
2. Find en post delt af Recleiner, som viser et billede af en måge.
3. Åben billedet og klik på "detaljer" for derefter at se exif data.
4. Gå til google maps og sæt GPS koordinaterne ind. For eksempel 55 41'34.0"N 12 35'56.6"E

THE CULTURAL CODE

I denne challenge er der fokus på at gennemskue slag af falske billetter.

Challenge-beskrivelse på Haaukins

A certain important "mister important" on peacock.hkn is going to a cultural event.

But the tickets might be fake. Go to peacock.hkn and find out.

Løsning:

1. Gå til peacock.hkn
2. Find en post, hvor Jens Bigboss poster et billede af 2 koncertbilletter.
3. Scan QR-koden på billedet med en telefon eller lignende og få flaget.
4. Flaget er HKN{TH34TOR-CULTUR3}

THE YELLOW SNITCH

Man har ofte mange informationer skrevet ned på post-it notes i kontormiljøer. Det skal man være opmærksom på, hvis man deler billeder af sin arbejdsplads. Denne opgave viser igen nogle af risiciene ved at dele billeder, hvor der optræder personlige oplysninger.

Challenge-beskrivelse på Haaukins

Office spaces can be filled with interesting information. The yellow snitches are always ready to share. Go to `peacock.hkn` and see if you can find any.

Løsning:

1. Gå til peacock.hkn
2. Find et billede af en kontorplads postet af Jens Bigboss.
3. Åbn billedet i et nyt browservindue og zoom ind.
4. Brug e-mailen og kodeordet på en af post-it-noterne til at logge ind på peacock.hkn.
5. e-mail: jens@hmail.hkn, password: YENEX2EC
6. Find flaget under profilsiden på Jens Bigboss' profil.

JOHNS WEIRD COMMENT!?

Denne opgave fokuserer på et lidt mere teknisk emne. Nemlig at information ikke altid står skrevet i normal tekst, men tit er base64 encoded, da dette format ofte bliver brugt til at repræsentere data på computere. Dette er også vigtigt at have in mente, når vi deler links.

Challenge-beskrivelse på Haaukins

Go to peacock.hkn and see if you can decode John's weird comment.

Løsning:

1. Gå til peacock.hkn
2. Find en mærkelig kommentar fra John Jensen under en af Ginas posts.
3. Brug en online decoder som f.eks https://dencode.com/en/ til at få flaget.

THE HASH HACK

Vores kodeord bliver normalt krypteret med en hashing algoritme eller lignende, når de bliver gemt på hjemmesider. Nogle algoritmer er mere sikre end andre. I denne opgave skal eleverne undersøge et md5-hash og finde ud af, at det har en del svagheder. Det er grunden til, at man bruger andre algoritmer i nye systemer til at gemme kodeord.

Challenge-beskrivelse på Haaukins

Someone from the criminal organisation is recruiting new members.

See if John can help you get through the recruitment challenges.

Go to peacock.hkn and solve the riddle.

Løsning:

1. Gå til peacock.hkn
2. Find en post, hvor Recleiner rekrutterer nye medlemmer til organisationen Anonymous sandworms.
3. Brug terminalværktøjet John til at bryde koden eller et andet online værktøj til at bryde hashet i.e https://crackstation.net/.
4. John: john --format=Raw-MD5 filename
5. Find Febrinas e-mailadresse inde på hendes profil.
6. Log in på Febrinas bruger og find flaget på hendes profil.

THE SUITCASE

Denne challenge er til de hurtige elever, som har løst alle de andre challenges. Fokus er her på, at man kan embedde filer i billeder. Dette kunne f.eks. være malware eller lignende.

Challenge-beskrivelse på Haaukins

Mister Beef is showing off his recent haul. Maybe a forensic tool like binwalk can help us find out what where he hid the money. Go to `peacock.hkn` and see if you can find out!

Løsning:

1. Gå til peacock.hkn
2. Find en post, hvor Mister Beef viser sit seneste grej frem (kuffert med penge)

3. Download billedet.
4. Brug terminalværktøjet binwalk til at se og udpakke gemte filer i billedet: bash
5. Find flaget i de udpakkede filer og voila, du har fundet flaget: HKN{W41Kin_Th3_B1n}

ROCKIES CODE

Denne challenge relaterer sig også til de informationer, som vi kan komme til at dele med hinanden igennem billeder. Denne gang er det kombineret med nogle ekstra elementer i form af, at vi også skal bryde et hash.

Challenge-beskrivelse på Haaukins

Miss Rockie er en meget struktureret person. Hun har en liste over alle fremtidige opgaver og aktiviteter for hver uge. Hun er også meget aktiv på de sociale medier og deler kalenderen med sine venner. Denne gang har hun delt noget meget vigtigt. Gå til `peacock.hkn/` og start med at få adgang til Miss Rockies' profil.

Løsning:

1. Find en post lavet af Miss Rockie ogse grundigt på billedet.
2. Find ud af, at der er en e-mailaddresse på billedet samt en post-it-note med et hash.
3. Bryd hashet med et online værktøj som f.eks. crackstation.net.
4. Hashet er "329670c3265b6ccd392e-622733e9772f"
5. Log ind på Miss Rockies' bruger med det fundne password og gå til hendes profilside for at finde flaget.

THE GRADUATION PARTY

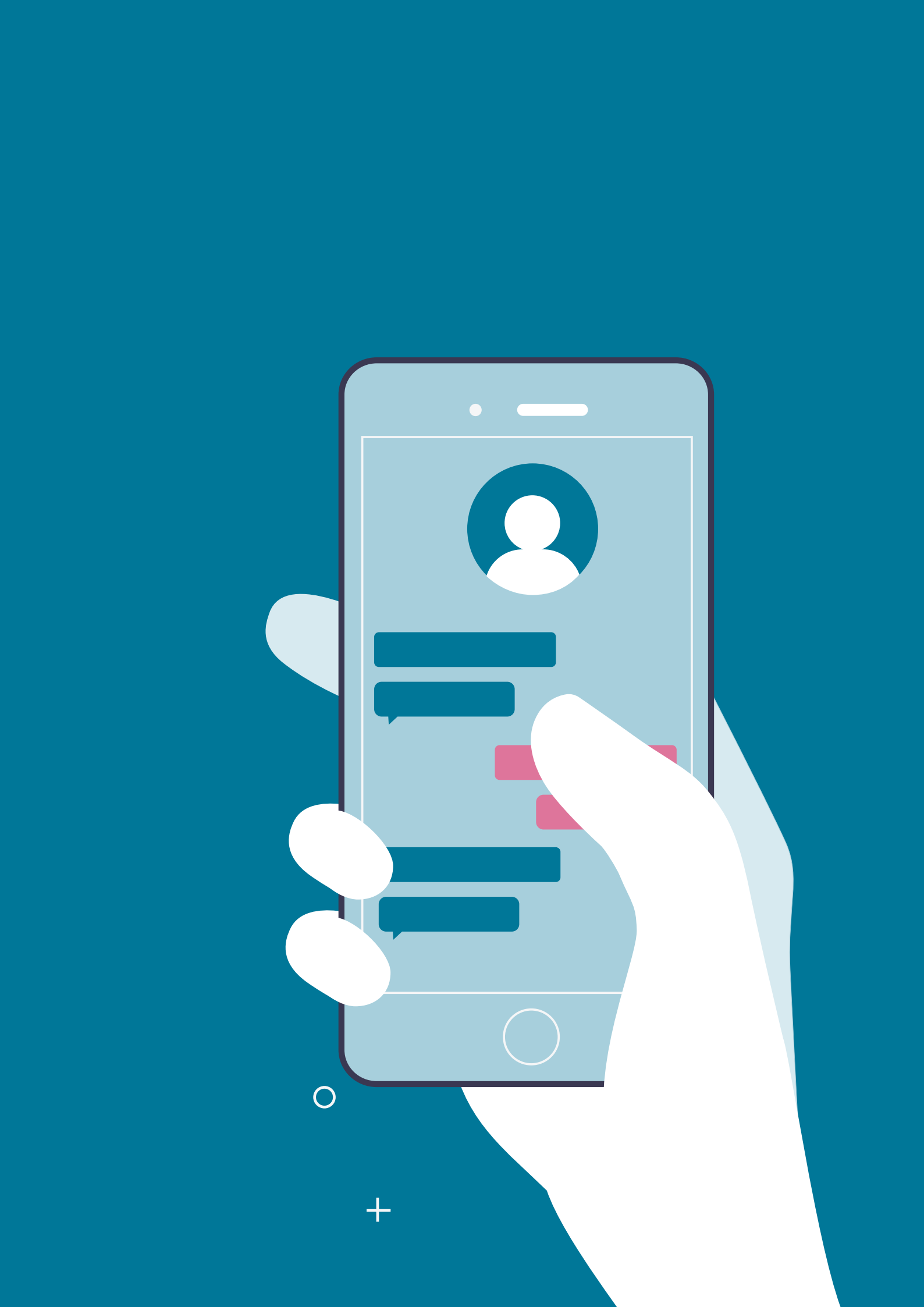
Denne challenge omhandler også de informationer, vi deler på billeder. Det er ikke bare login-oplysninger og lokation, vi kan dele på vores billeder, men også andre personfølsomme oplysninger.

Challenge-beskrivelse på Haaukins

Miss Rockie is so happy to defend her Ph.D. She is so proud of her achievements! See if you can find her CPR number and date of graduation. Go to `peacock.hkn/` and find out. Flag format: HKN{date_cpr} EX: HKN{22012022_080904-8843}

Løsning:

1. Find Miss Rockies' post af et eksamensbevis.
2. Find hendes CPR-nummer under hendes navn og dimensionsdato i højre hjørne af dokumentet.
3. Flaget er HKN{11012022_010134-5678}



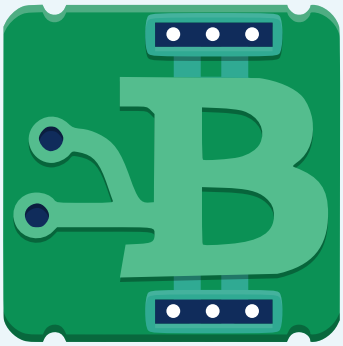
VÆRKTØJSKASSEN

ExifTool

NMAP

HYDRA

in Kali linux machine

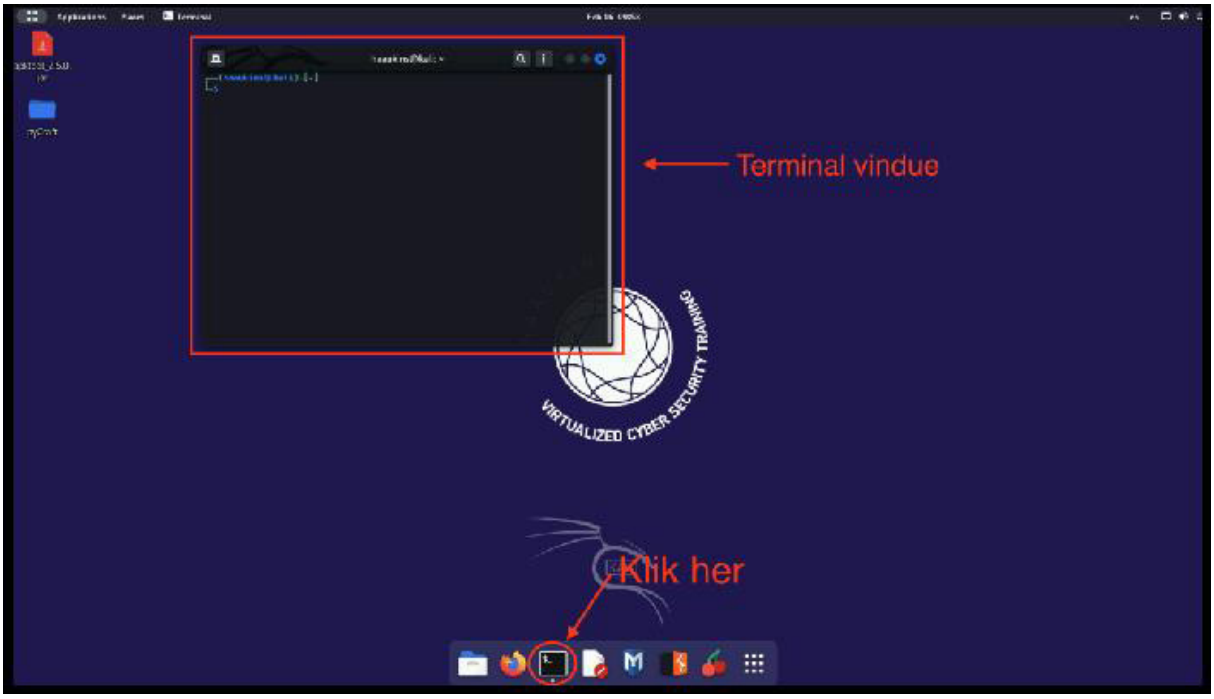


WIRESHARK

VÆRKTØJSKASSEN TIL ELEVER OG LÆRER

Dette er en værktøjskasse med et par gængse værktøjer, som du vil få brug for til nogle opgaver på platformen Haaukins. Alle værktøjer, som skal bruges til opgaverne, er allerede installeret på den virtuelle Linuxmaskine. For at bruge nogle af værktøjerne, skal vi bruge et terminalvindue. Husk, at alle værktøjer beskrevet herunder kan rigtig mange ting. Derfor vil det altid være en god idé at bruge lidt tid på at søge lidt på internettet eller lignende, inden man bruger de forskellige værktøjer.

For at kunne bruge værktøjer og alle elementer herunder skal man være logget ind på platformen Haaukins. I finder en kort video til, hvordan I kommer i gang med Haaukins under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/



TERMINAL

For at få adgang til værktøjerne skal vi åbne et terminalvindue. Det kan gøres ved at klikke på følgende ikon:
For at navigere mellem mapper i terminalvinduet kan vi bruge følgende kommandoer:
$ ls # Vis, hvilke filer vi kan se i den mappe, vi er i.
$ cd # Bruges til at gå over til en anden mappe.

---------- EKSEMPEL ----------

$ cd Downloads # Gå til Downloads
$ ls # Vis filer, der ligger i Downloads
$ cd # Gå tilbage til start
$ cd .. # Gå en mappe op i mappehierakiet.

Prøv at taste ovenstående ind i dit eget terminalvindue.

BINWALK

Binwalk er et værktøj, som kan søge i en given fil efter indlejrede filer. Det kan være brugbart i situationer, hvor man gerne vil finde ud af, om der er ekstra filer med i f.eks. et billede. Binwalk er et terminalprogram. Det vil sige, at for at bruge værktøjet skal man åbne terminalen, navigere til den mappe som filen, man gerne vil undersøge, ligger i, og derefter skrive binwalk efterfulgt af navnet på den fil, man gerne vil undersøge.

For eksempel:

- $ cd Downloads # Gå til downloads
- $ ls # Vis filnavnene på filer i downloads
- $ binwalk billede.jpg # Brug binwalk til at undersøge en fil.

For at læse mere om binwalks mange funktionaliter, kan man søge på det, på nettet.

EXIFTOOL

ExifTool er et værktøj, som kan vise exif-data, som ligger indlejret i billeder. For at bruge ExifTool på et billede, kan man gøre følgende i terminalen:

- $ cd Downloads # Gå til downloads
- $ ls # Vis filnavnene på filer i downloads.
- $ exiftool billede.jpg # Brug exiftool til at undersøge en fil

For at læse mere om ExifTool, kan man søge det på nettet.

JOHN THE RIPPER

John the ripper (John) er et meget fleksibelt værktøj, som kan bryde koder. Værktøjet understøtter både brug af ordlister og brute-force angreb. Man sørge for at få konverteret filen, som man gerne vil bruge John på, til det rigtige format. For at bruge værktøjet skal man åbne terminalen og navigere til den mappe, som filen, man gerne vil arbejde på, ligger i. F.eks.

- $ cd Downloads # Gå til downloads
- $ ls # Vis filnavnene på filer i mappen
- $ john filnavn # Brug john til at bryde en kode

HYDRA

Hydra er et værktøj lavet til at bryde kodeord til servere som f.eks. FTP-servere, som også findes i dit terminalvindue. Det er også et rigtig multifunktionelt værktøj, som du kan læse mere om, hvordan man bruger, det på nettet.

NMAP

Vi går fluks videre til et andet cool værktøj, som hedder NMAP. Det kan bruges til at scanne det netværk, man sidder på, eller andre services på nettet. Herunder er et eksempel på, hvordan man kan bruge NMAP til at skanne sit netværk og se, hvilke enheder der er online på det subnet, vi scanner:

- $ ifconfig # Bruges til at finde din egen IP.
- $ nmap 192.162.3.14 # Scan af en enkelt host.
- $ nmap 192.162.3.14/24 # Scan af et helt subnet.
- $ nmap -O 192.162.3.14 # Scan af en enkelt host med fingerprint.

Da NMAP har rigtig mange funktionaliteter, er det altid en god idé at læse lidt op på værktøjet på nettet f.eks: https://cybertraining.dk/network_scanning/#/ eller søg på google.

Usage	Filter syntax
Filter by IP	ip.addr == 10.10.150.1
Filter by destination IP	ip.dest == 10.10.150.1
Filter by source IP	ip.src == 10.10.150.1
Filter by port	tcp.port == 25
Filter by destination port	tcp.dstport == 23
Filter by domain name	http.host == “domain.hkn”

WIRESHARK

Wireshark er et værktøj, som kan bruges til at lytte med på det lokale netværk. Herunder er en masse kommandoer, som kan bruges i Wiresharks søgefelt til at filtrere den internettrafik, som man har opsamlet:

Logical operators

Operator	Description	Example
and / &&	Logical AND	All the conditions should match
or / ||	Logical OR	Either all or one of the conditions should match
xor / ^^	Logical XOR	Only one of the two conditions should match
not / !	Logical NOT	Not equal to

For at lave mere avancerede filtre kan man bruge både **Logical operators** samt **Filter operators:**

Filter operators

Operator	Description	Example
eq / ==	Queal	ip.dest == 192.168.1.1
ne / !=	Not equal	ip.dest != 192.168.1.1
gt / >	Greater than	frame.len > 10
lt / <	Less than	frame.len < 10
ge / >=	Greater than or equal	frame.len >= 10
le / <=	Less than or equal	frame.len <= 10

Hvis du er nysgerrig på mere, er følgende link et godt sted at starte: https://cybertraining.dk/metasploit_0/#/ eller søg på nettet.

System navigation

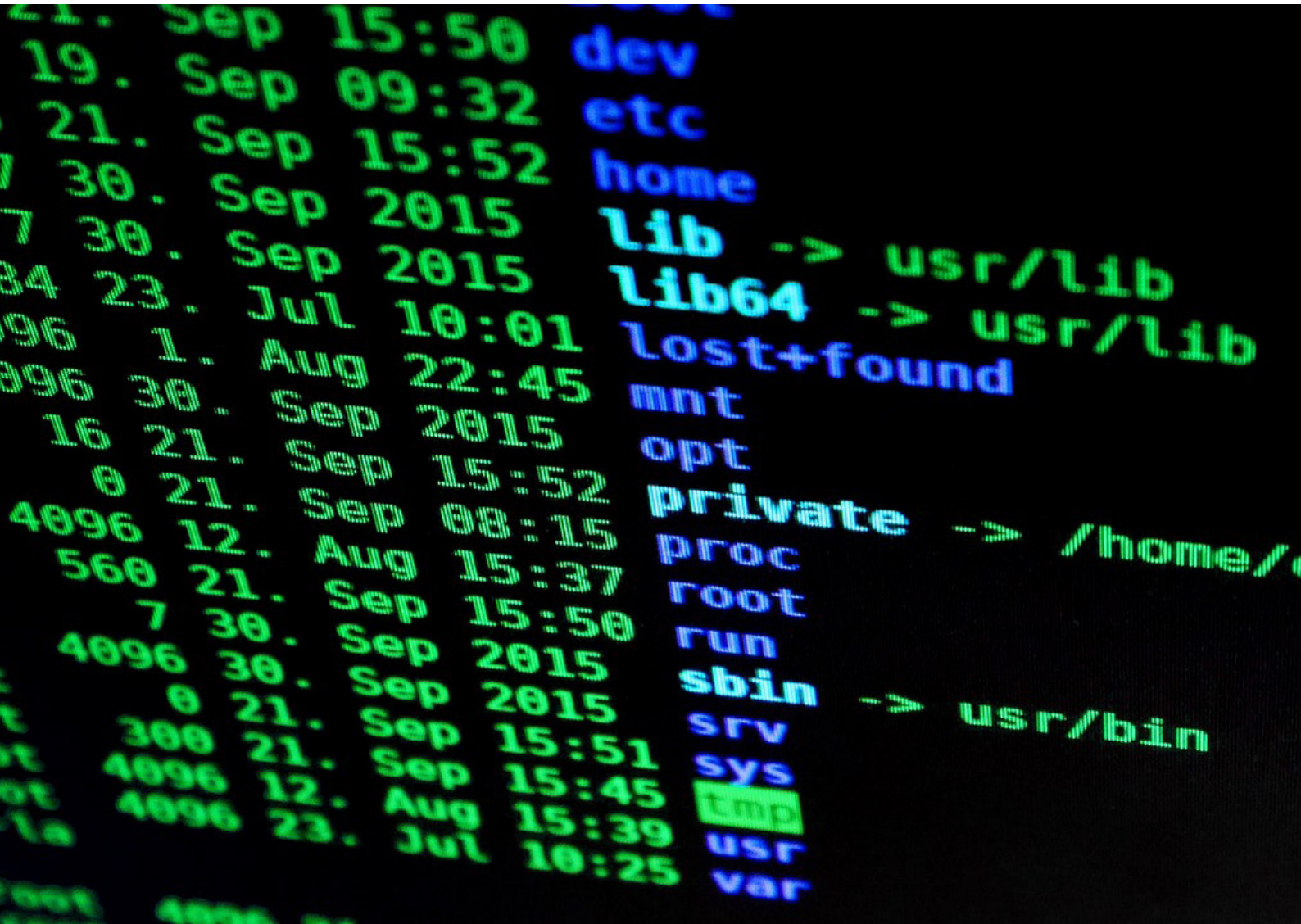
Description	Command
Ssh to host	ssh <user>@<network_domain_name>
Switching user	su <username>
List files and directories	ls
List files and directories (including hidden)	ls -a
Changing directory	cd <directory_name>
Filter by domain name	http.host == “domain.hkn”

Interacting with files

Description	Command
Creating new file	touch <filename>
Creating new directory	mkdir <directory name>
Moving file/directory	mv <file or directory name> <Destination path>
Copying file/directory	cp <file or directory name> <Destination path>
Reading contents of file	cat <filename>
Search for a specific text string in file	grep “string_to_search_for” <filename>
Writing to a file	myCommand > filetowriteto.txt

Permissions and complex commands

Description	Command
Find a file in directory tree	find <root_of_search> -name “filename”
Reading network information	ifconfig
Chaining commands	<command 1>
Changing permissions of file	chmod <permissions> filename.txt
Reading contents of file	cat <filename>
Executing files	./<filename>



CYBERMISSIONEN

BEGREBSLISTE

Hvor mange begreber kender I?

TRUSSELSMODELLERING

Trusselsmodellering handler kort fortalt om at identificere sårbarheder i et system og dermed også uønskede hændelser, så man eksempelvis som udvikler af et stykke software kan være bedre forberedt.

COOKIES

En cookie er en fil, der bliver gemt på din computer, når du besøger en hjemmeside. Nogle cookies er nødvendige for at hjemmesiden virker, andre husker hvad du klikker på, så hjemmesiden kan sende reklamer, som passer til dig. Når du besøger en hjemmeside, kan du vælge hvilke cookies du vil acceptere.

CYBER AWARENESS

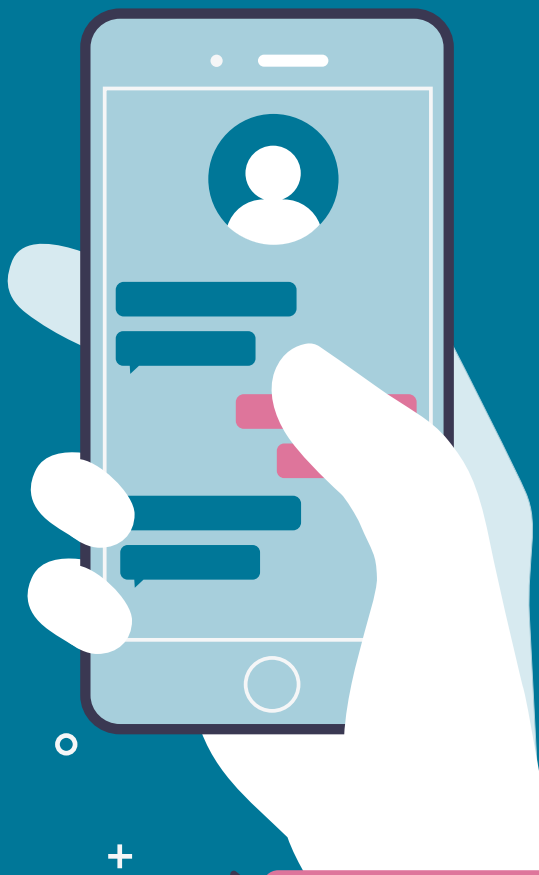
Mange virksomheder laver cyber awareness træning. Det kan eksempelvis være kommunikationsaktiviteter eller uddannelse, der skaber opmærksomhed om informationssikkerhed hos medarbejderne, så de får en mere sikker digital adfærd.

DIGITALE FODSPOR

Når du søger på Google, sender en snap eller uploader en video på TikTok efterlader du dig spor på nettet, som bliver gemt. Det kaldes digitale fodspor, og de kan være meget svære at slette igen.

HACKING

Hacking er, når nogen ulovligt skaffer sig adgang til andres data - eksempelvis via en computer. Hackere udnytter svagheder i systemer. En svaghed kan eksempelvis være passwords, der er nemme at gætte.



DDOS-ANGREB

DDos-angreb står for Distributed Denial of Service. Det er et digitalt angreb, hvor en hacker med vilje overbelaster en hjemmeside eller en it-service, så siden i en periode er utilgængelig eller bryder helt sammen. Angrebet udføres ved, at hackeren gennem et netværk af virusinficerede computere, et såkaldt botnet, sender en stor mængde forespørgsler til hjemmesiden og dermed får siden til at bryde sammen.

VULNERABILITY DISCLOSURE PROGRAM

En VDP giver etiske hackere klare retningslinjer for, hvordan de indberetter potentielt ukendte
og skadelige sårbarheder til de organisationer, der står bag systemet.

TO-FAKTOR LOGIN

To-faktor login er en dobbelt lås, som typisk består af dit password og en kode, du får tilsendt - ofte på sms. Hvis andre får fat i dit brugernavn og password og forsøger at logge ind på din konto, kan det derfor ikke lade sig gøre, fordi de mangler den anden kode, som er sendt til din mobil.

TROLL

En troll (på dansk: internettrold) er en person, som bevidst forsøger at fremprovokere vrede og had på internettet.

RISIKOANALYSE

En risikoanalyse er et værktøj, som har til formål at afdække potentielle risici ved at kategorisere dem ift. den mulige konsekvens og sandsynlighed for, at de indtræffer. Risikoanalysen anvendes dernæst til at prioritere ressourcer og beslutte hvilken handling, der skal sættes ind for at sikre, at det ikke går galt.

PHISHING

'Phishing' er, når it-kriminelle bruger falske e-mails, links eller hjemmesider til at få fat i andres private oplysninger, eksempelvis til banken. Det er tit svært at se forskel på, hvad der er falske links, mails og hjemmesider, og hvad der er ægte.

Artefakt

Kan I finde flere ord?

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING

CYBER SKILLS

Cybermissionen - NOTER

Cybermissionen - NOTER

Cybermissionen - NOTER

Cybermissionen - NOTER

CYBERMISSIONEN

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING

CYBER SKILLS