CYBERMISSIONEN

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

CYBER SKILLS

CYBERMISSIONEN

ISBN nr:
87-603-3343-X (trykt udgave)

Design:
Børne- og
Undervisningsministeriet

Børne- og Undervisningsministeriet
Styrelsen for It og Læring
Vester Voldgade 123
1552 København V

INDHOLDSFORTEGNELSE

MISSION 1: CYBER AWARENESS SIDE 4-8

FLERE UNDERSØGELSER VISER, AT MANGE IKKE ALTID GØR DET, DE GODT VED, DE BURDE GØRE I FORHOLD TIL DATASIKKERHED. I DENNE MISSION SKAL I LAVE EN KAMPAGNE, SOM I MENER STYRKER JERES MÅLGRUPPES CYBER AWARENESS, SÅ DE BLIVER MERE SIKRE PÅ NETTET.

MISSION 2: PRIVACY OG CYBERMOBNING SIDE 9-13

DENNE MISSION HANDLER OM GOD CYBERHYGIEJNE OG OM AT KONTROLLERE OG SIKRE SINE INFORMATIONER OG SIT PRIVATLIV ONLINE. I SKAL ARBEJDE MED EN CASE OM ANNA, SOM OPLEVER AT ALTING GÅR HELT AMOK PÅ NETTET OG AT HUN IKKE HAR KONTROL OVER SINE PERSONLIGE OPLYSNINGER.

MISSION 3: TÆNK SOM EN HACKER SIDE 14-19

I DENNE MISSION SKAL I ARBEJDE MED DET, SOM KALDES "ETISK HACKING". I ET SIKRET MILJØ SKAL I TRÆDE I HACKERNES FODSPOR FOR AT BLIVE KLOGERE PÅ, HVORDAN DE TÆNKER, SÅ I PÅ DEN MÅDE BEDRE KAN MODSTÅ DERES ANGREB.

MISSION 4: GØR DET MULIGT AT VÆRE EN GOD HACKER SIDE 20-22

I DENNE MISSION SKAL I DYKKE NED I, HVORDAN VIRKSOMHEDER KAN SKABE DE RETTE RAMMER FOR ETISK HACKING OG DERMED BIDRAGE TIL AT STYRKE DERES EGEN IT-SIKKERHED.

MISSION 5: (U)SIKKERHED I SMART HOME ASSISTANTS SIDE 24-27

AMAZON ALEXA, GOOGLE ASSISTANT OG APPELS SIRI ER EKSEMPLER PÅ SMART HOME ASSISTENTER VI HAR INVITERET IND I VORES HJEM. I DENNE MISSION SKAL I PILLE EN SMART HOME ASSISTENT FRA HINANDEN, IDENTIFICERE SÅRBARHEDER I SYSTEMET OG DERVED OGSÅ MÅDER HVORPÅ DEN KAN HACKES.

BEGREBSLISTE SIDE 28

I BEGREBSLISTEN FINDER I KORTE DEFINITIONER PÅ NØGLEBEGREBER I MATERIALET.

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: 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, 'små handlinger' kan lede til.

It-sikkerhed er et vigtigt område, der skal mere fokus på, og det er det, 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 kommunikationskampagnen. 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 KOMMUNIKATIONSKAMPAGNEN 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 mm.

GODE RÅD TIL KAMPAGNEUDFORMING

Når I skal i gang med at lave selve kampagnen, er det en god ide 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

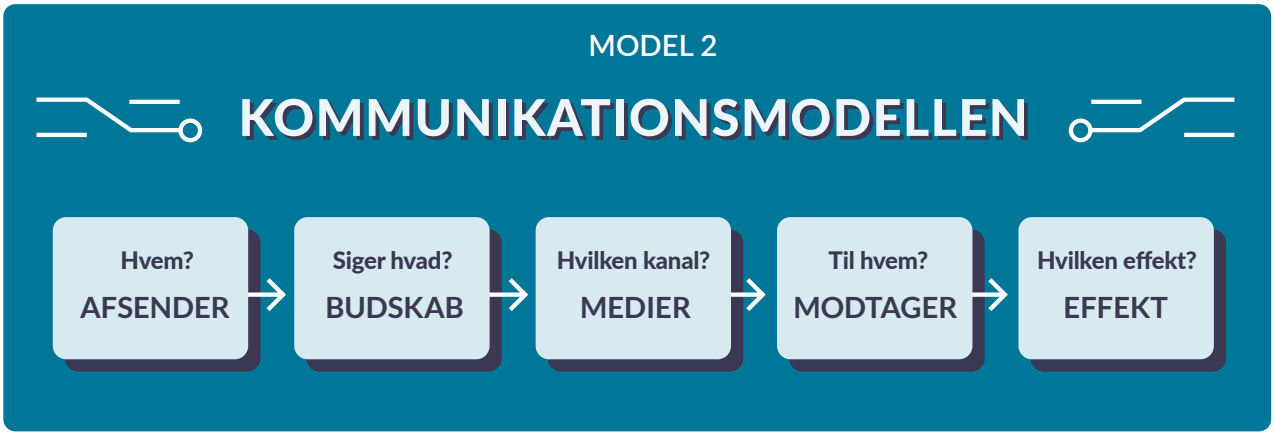
ETOS, LOGOS OG PATOS

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 I får 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/

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 ind 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 2: PRIVACY OG CYBERMOBNING

Har du nogensinde følt, at ting er gået helt amok på nettet og du ikke havde kontrol over dine personlige oplysninger? Denne mission handler om at kontrollere og sikre dine informationer og dit privatliv online.

DINE DATA PÅ NETTET

Vi bruger vores personlige data hver dag, for eksempel på hospitaler, i skolen og når vi er i kontakt med forskellige virksomheder. Vi deler også informationer om vores liv, fritid og færden på spilsider, sociale medier og apps. Det er med andre ord umuligt at gå gennem hverdagen uden, at der bliver opsamlet data om en.

Vores aktiviteter online overvåges, gemmes og analyseres af både firmaer og offentlige myndigheder. Gennem den data de opsamler får de viden om deres brugeres adfærd og behov, så de kan udvikle og forbedre de services de sælger eller stiller til rådighed.
Der er altså en række gode grunde til at dataopsamlingen sker, men det medfører også den risiko, at dataen kan blive misbrugt. Som denne mission afslører, er det ikke kun virksomheder, der kan bruge den data, der er tilgængelige om os på nettet – den kan også bruges af private personer.
Det er derfor vigtigt at skabe en bevidsthed om privatliv blandt alle, også unge mennesker. Denne mission skal få jer til at tænke over, hvordan I kan beskytte jeres private data, hvordan I kan surfe på internettet uden at efterlade jer spor, og hvordan I kan forblive anonyme på internettet. I skal som del af missionen lære om "cyberhygiejne" det vil sige, hvordan du beskytter dit privatliv online. Men det kræver, at I selv bruger jeres research-evner til at finde svarene.

Inden I går i gang med missionen kan I se en introvideo om trolling og digital chikane. I finder videoen under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/

JERES MISSION

Mission 2 fokuserer på personer, der forfølger andre personer online. I skal arbejde med og reflektere over vigtigheden af at være forsigtig på nettet, overveje etikken og den potentielle skade, cybermobning kan gøre.

Vigtigst af alt sætter missionen fokus på, hvorfor gode vaner for cybersikkerhed og privatliv online er vigtigt. Vi håber at missionen kan inspirere jer til gode overvejelser og give jer ny viden om god cyberhygiejne.

Missionen er inddelt i tre sektioner. Der er spørgsmål undervejs som I skal tænke over og tale om for at kunne besvare dem. Til sidst skal I opsummere det hele i et kommunikationsprodukt, eksempelvis en plakat.

TEENAGER BLIVER OFFER FOR TROLL-ANGREB

I vil få præsenteret en case, der gennemgår historien om en teenager, der bliver mål for cybermobning efter, at hendes post på Instagram går viralt.

Casen begynder med, at mobningen kun sker på de sociale medier. Men det eskalerer gradvist til at påvirke offeret og hendes familie også i den fysiske verden.

Situationen kommer mere ud af kontrol, da mobberne får adgang til hendes konti, og hun bliver offer for cyberkriminalitet.

Denne case er fiktion, men den er lavet ved at kombinere elementer fra flere virkelige historier. Så det kunne faktisk have været dig, din ven eller din nabo.

CASEN

ANNAS OPSLAG PÅ INSTAGRAM RESULTERER I TROLL-ANGREB

Anna er en typisk gymnasieelev i Danmark. Hun har et godt socialt liv og er aktiv på flere sociale medier.

Annas 500 Instagram-følgere er mest hendes venner, folk fra samme skole og hendes familie. Hendes konto er ikke privat, men nærmest ingen udenfor hendes sociale cirkel liker eller deler det, hun poster.

DEL 1

EN POST GÅR VIRALT PÅ SOCIALE MEDIER, OG MOBNINGEN BEGYNDER

En dag poster Anna et foto på Instagram med en joke om et populært fodboldhold, der lige har tabt til hold, der normalt ikke klarer sig særligt godt – hun knytter et par hashtags til billedet. Hun tænker ikke så meget over indholdet og har faktisk ikke engang stærke følelser omkring det. Men hun deler det, fordi hun synes, at det er sjovt.

Flere dage senere går en populær influencer, som Anna hverken kender eller følger, gennem posts med et af de hashtags som Anna brugte til sit opslag. Influenceren ser fotoet med joken og bliver irriteret over det. Influenceren deler et screenshot og Annas profilnavn på Instagram. Nu kan over 100.000 mennesker se Annas post, hvilket er 200 gange flere end dem, der normalt ser hvad Anna poster på Instagram – og dermed også mange mennesker, som Anna slet ikke havde tænkt skulle se joken.

Næste morgen vågner Anna op til tusindvis af notifikationer på sin mobil. Hendes profil får pludselig besøg af tusindvis af mennesker – såkaldte trolls/trolde - der kommenterer på hendes nuværende og gamle posts. Mange deler influencerens screenshot med kommenterer med alt fra fornærmelser som ”dumme tøs” til trusler om at ”hun burde skydes”.

Anna skynder sig at slette det oprindelige foto, men folk holder ikke op med at kommentere, og de går videre til hendes ældre posts. Anna ender med at gøre sin profil privat og ændrer kontonavnet for at stoppe dem.

Men raseriet stopper ikke der. Der er stadigvæk trolls, der sender Annas posts i omløb, deler screenshots af hendes posts med kommentarerne og laver nye hashtags om at “cancel” hende. Det lykkedes også for dem, der chikanerer Anna, at identificere hendes kæreste og flere nære venner ud fra Annas billeder, hvilket betyder at de nu også bliver chikaneret af ”troldene”.

ARBEJDSSPØRGSMÅL

HVORDAN AFVÆRGER MAN BEDST ET TROLL-ANGREB?

Arbejdsspørgsmål til del 1:

1. Lav en liste over de ting, der førte til troll-angrebet mod Anna, hendes kæreste og venner.
2. Sortér listen mellem de ting, som Anna selv har kontrol over og de ting, der er udenfor hendes kontrol.
3. Hvad kunne Anna have gjort anderledes for at undgå troll-angrebet?
4. Hvad skal Anna gøre nu, hvor chikanen fortsætter?
5. Hvor går grænsen for jokes?
   Det kan være svært, at forstå, hvorfor så mange folk begynder at chikanere Anna. Men det, som virker som en sjov og ufarlig joke for en person, kan virke voldsomt og helt urimeligt på en anden person. Prøv at lave nogle eksempler på jokes om for eksempel et fodboldhold, og diskuter hvilke I selv ville have lyst til at dele på sociale medier – og hvilke I tænker er over grænsen. Ser I forskelligt på det? Og er der forskelle på, hvad I vil dele hvor og med hvem?

TIP: Tænk på, hvorvidt internettet er et frit miljø, hvor alle skal have lov til at dele deres meninger - og om I synes, at folk har ret til at svare Anna? Hvor går grænsen mellem at udtrykke sig og at chikanere? Og hvor går grænsen mellem, hvad der en sjov joke og hvad der er mobning?

DEL 2

CHIKANEN NÅR DEN VIRKELIGE VERDEN

Ukendte personer fra internettet får opsporet Annas fulde navn, og ved at google og **søge forskellige steder**, finder de frem til Annas telefonnummer, e-mailadresse, og hvor hun bor. Annas kontaktoplysninger bliver delt i et anonymt online-forum, og de spredes mellem de mennesker, der var rasende over hendes oprindelige post om fodboldholdet.

Det betyder, at Anna begynder at blive ringet op af folk, hun ikke kender, hvilket hun heldigvis kan stoppe ved at få nyt telefonnummer. Men hun oplever også chikane i form af, at få leveret pizza, hun ikke har bestilt - og der bliver kastet skrald på hendes vinduer. Mest alvorligt er, at hun får flere dødstrusler sendt med posten.

Tingene når kogepunktet, da en person ringer til Annas far og udgiver sig for at være fra politiet. Annas far opdager hurtigt, at det ikke er en rigtig politibetjent og råber af personen i ren frustration. Hans reaktion bliver optaget og bagefter bliver Annas fars svar, som er fyldt med bandeord, lagt på internetsiden 4chan. Troldene glæder sig over mandens vrede, og Annas far bliver brugt som internetmemes.

Nu får hele familien nye hemmelige telefonnumre.

ARBEJDSSPØRGSMÅL

1. Hvordan tror I, at troldene kunne de finde Annas privatadresse?
   - *Lav en liste over alle de steder og spor, der kan bruges til at finde frem til hvor en person bor.*

TIP: Husk, at alt, hvad vi gør online, efterlader et spor. Posts, der ser uskyldige ud, kan bruges til at identificere privat information.

2. Hvad kunne Anna have gjort for at begrænse udbredelsen af hendes personlige oplysninger?

TIP: Undersøg hvad nøglebegreber som doxing og oversharing betyder.

"1 UD AF 7 DANSKERE MELLEM 18 OG 34 HAR OPLEVET AT BLIVE CHIKANERET ELLER STALKET PÅ NETTET"

(Userneeds, ingeniørforeningen IDA, 2017)

3. Hvad skal Anna gøre nu, hvor fremmede truer hende og hendes familie?

TIP: Undersøg hvem, der kan hjælpe familier i samme situation som Annas (myndigheder og andre) og hvad de anbefaler at man gør.

DEL 3

UAUTORISERET ADGANG

Anna har ikke været særlig opmærksom på sikkerhed online, og har brugt den samme, meget simple, adgangskode til alle sine konti. Et af de steder, hvor Anna har brugt sin adgangskode, er et online forum – der i en helt anden situation, som ikke har noget med troll-angrebet på Anna at gøre, har været offer for hacking. Hackerne delte kontonavne, e-mailadresser og adgangskoder for tusindvis af mennesker i flere fora, og nu er Annas kontoinformationer pludselig interessante for troldene at finde. På grund af hacket og det, at hun brugte den samme adgangskode overalt, kan enhver finde både hendes e-mailadresse og adgangskode med en googlesøgning.

Troll-angrebet bliver udvidet, da angriberne finder og bruge den samme adgangskode til at få adgang til Annas e-mailkonto. Ved at se på kontoens e-mailhistorik kan angriberne også se, hvilke sider og apps hun er registreret på. Anna har blandt andet en Snapchatkonto, som angriberne nu kan bede om at få et nyt kodeord til, fordi de kender hendes e-mailadresse. Efter de får den nye kode, har angriberne fri adgang til kontoen, og kan også ændre oplysningerne.

Troldene kan nu se alle Annas private beskeder, fotos og aktivitetslog og de spreder det hele online. De finder også nogle personlige intime billeder på de konti, som kun var til hende og hendes kæreste. Nu bliver de sendt i omløb online.

ARBEJDSSPØRGSMÅL

1. Bruger I den samme adgangskode til flere konti? Hvorfor?
2. Hvordan kan man sikre sine konti endnu bedre?

TIP: Undersøg hvad password managers, multi-faktor-login og to-faktor-login er, og hvad det betyder for at have en god cyberhygiejne.

3. Hvilke typer konti, kan man oprette?
   - lav en liste over de mange forskellige typer konti, som I tænker Anna, jer selv og andre unge nok har adgang til.
4. Er der forskel på hvilke konti, det er vigtigt at beskytte adgangen til? Er der nogen hvor sikkerhed og forsigtighed er vigtigere end andre? Undersøg hvad den gamle talemåde "kæden er aldrig stærkere end sit svageste led" betyder, og tænk over, om det er relevant at bruge talemåden i en tid med online konti og adgangskoder.

BRUG JERES VIDEN TIL EN INFORMATIONSKAMPAGNE

For at løse mission 2 skal I lave en informationskampagne – det kan eksempelvis være en plakat. I skal bruge den viden I har opsamlet i jeres arbejde med casen om Anna og troll-angrebet til at lave en plakat (eller et andet kommunikationsprodukt), der kan hjælpe andre til at få en bedre cyberhygiejne.

INSPIRATION TIL BUDSKABER

I må selv bestemme, hvilket budskab I synes er det vigtigste at kommunikere.

I kan bruge følgende to eksempler til inspiration, eller finde på jeres eget:

1. Kampagnen skal få folk til at overveje, hvilke informationer de deler på sociale medier.
   Eller
2. Kampagnen skal få de trolde, der måske uden at tænke over det "mobber" online – til at overveje deres adfærd.

Forhåbentlig kan vi med jeres ideer til gode kampagner, nedsætte antallet af sager som Annas i fremtiden.

JERES PRÆSENTATION

I skal nu forberede en præsentation af jeres arbejde med missionen og jeres produkt.
I præsentationen skal I:

- Kort redegøre for jeres mission, den viden I har fået og de refleksioner I har gjort jer omkring Annas case.
- Præsentere jeres informationskampagne (gerne med billeder, video, skærmoptagelse m.m.)
- Fortælle, hvordan I kom frem til jeres endelige informationskampagne
- Argumentere for, hvilken effekt I tror, at jeres kampagne kan få hos jeres målgruppe
- Fortælle, hvilke refleksioner eller ahaoplevelser, I har haft undervejs
- 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 ind 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 upload funktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.

MISSION 3: TÆNK SOM EN HACKER

Du har måske hørt om den forhøjede trussel, der er overfor specielt kritisk infrastruktur i Danmark lige nu. Kritisk infrastruktur omhandler sektorer som: sundhedssektoren (herunder hospitaler), energisektoren, IT- og teleområdet, transportsektoren og fødevareområdet. Der er frygt for, at hvis et eller flere af områderne udsættes for hackerangreb, kan dele af det danske samfund bryde sammen.

Det kan have store konsekvenser at blive udsat for et hackerangreb, uanset om man er et transportfirma eller en gymnasieelev. Derfor er det vigtigt at få indsigt i, hvordan cyberkriminelle arbejder, da det giver bedre forudsætninger for at modstå angreb.

HVIS MAN VED, HVORDAN DE CYBERKRIMINELLE ARBEJDER, ER DET LETTERE AT BESKYTTE SIG

Der er mange forskellige veje til at få adgang til en computer, et netværk eller lignende. Typisk gør hackerne det, at de leder efter smuthuller i den måde et stykke software, et netværk eller en computer er sat op på. De ser med andre ord på, hvor svaghederne i systemarkitekturen er, og de forsøger så at finde det svageste punkt og planlægge, hvordan de kan udnytte det til egen fordel. Hackere bruger deres viden om svaghederne til at bryde ind i systemerne og tiltvinge sig adgang til data eller andet som er af interesse. Ydermere arbejder de cyberkriminelle også med at finde sårbarheder, så de kan blokere andres adgang til systemet og måske endda omdirigere til et andet system (for eksempel en falsk hjemmeside), som brugerne tror er den rigtige. På den måde kan man let blive snydt.

JERES MISSION

I denne mission skal I arbejde som hackere for at forstå, hvilke typer af sårbarheder, man som hacker kan lede efter, når man vil finde et godt sted at slå til. Ligeledes skal I reflektere over, hvad I lærer, og se om I kan finde eksempler på løsninger, som allerede bruges. Der arbejdes i denne mission med det, som kaldes "etisk hacking". I skal bruge en virtuel platform som hedder Haaukins, hvor man kan tillade sig at hacke, uden at det kommer ud i den virkelige verden og bliver til en kriminel handling. Man må ALDRIG hacke rigtige hjemmesider, profiler på sociale medier osv., - det er ulovligt! Missionen har et teknisk element og vi anbefaler, at du har motivation for at arbejde med teknologi, programmering (i det små) og forstå lidt om hvordan internettet virker og hvordan IT-systemer er opbygget.

I denne mission skal I udarbejde tre forslag til sikkerhedstiltag, på baggrund af de erfaringer I får når I selv skal prøve at hacke og forberede en præsentation af dem.

MISSIONENS 4 TRIN

På trin 0 lærer I om Haaukins-platformen, som er den digitale cybersikkerhedsplatform, I skal bruge til etisk hacking.
På trin 1, 2 og 3 arbejder I med eksempler på sårbarheder. I bruger Haaukinsplatformen til at forsøge at hacke jer til løsninger mens I reflekterer over, hvad I har lært og hvordan de sårbarheder I ser, kan undgås.

TRIN 0

LÆR HAAUKINS PLATFORMEN AT KENDE

På trin 0 skal I lære om Haaukins-platformen, hvordan den ser ud og hvordan man navigerer på den. I skal også lære om Linux, som er det operativsystem, man bruger på platformen. Eksempler på andre operativsystemer er Windows og MacOS.

For at kunne arbejde med Haaukins, 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 (*Challenges*) og vælg den første challenge i kategorien "Starters" ved navn "List and Read". 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 en terminal (Kan findes i bjælken i bunden af det virtuelle lab) og følge de instruktioner, som nævnes i udfordringens beskrivelsen. Når I har løst den første opgave skal I løse de næste opgaver i rækkefølge. Følg ellers vejledningen på skærmen. Google er jeres ven! Når alle opgaver er løst, kan I starte på de egentlige opgaver i trin 1-3.

I finder en kort video til, hvordan I kommer i gang med Haaukins under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/

TRIN 1

LOG PÅ HAAUKINS PLATFORMEN OG LAV 2 OPGAVER

På trin 1 får I indblik i, hvad det vil sige at udføre etisk hacking. I lærer om de forskellige muligheder cyberkriminelle har for at hacke et system. I den challenge, der hedder *Cookiesession*, skal I lede efter cookies og se, om der er information i dem, der kan bruges til noget. Og i den challenge, der hedder *Adminlogin* skal I se, hvad der er af muligheder, når man har forsøgt at sætte lidt cybersikkerhed op, men kun har gjort det i cookies.

Når I har løst begge challenges, skal I reflektere over, hvad I har lært og hvilke løsninger, der kan være til at forhindre, det I lige har gjort.

TRIN 2

GIV ET BUD PÅ, HVAD CYBERKRIMINELLE SØGER EFTER

Løs nu den challenge, der hedder: *Cross site request forgery*, hvor man skal forsøge at hacke en bank.

Når denne challenge er løst, skal I tænke over, hvad I har lært af denne opgave, samt om I kan pege på sikkerhedsforanstaltninger, som kan forhindre pengebedrageriet.

TRIN 3

UNDGÅ HACKING – HVORDAN?

Løs nu den sidste challenge med navnet: *FTP server Login*, hvor man skal forsøge at gætte et password. Kan denne challenge bruges til at forstå, hvad man kan gøre for at reducere sandsynligheden for hacking? Prøv at snakke om hvorvidt to-faktor-login kan være en måde at sikre, at dette ikke sker. Begrund svarene.

BAGGRUND FOR TRIN 1-3

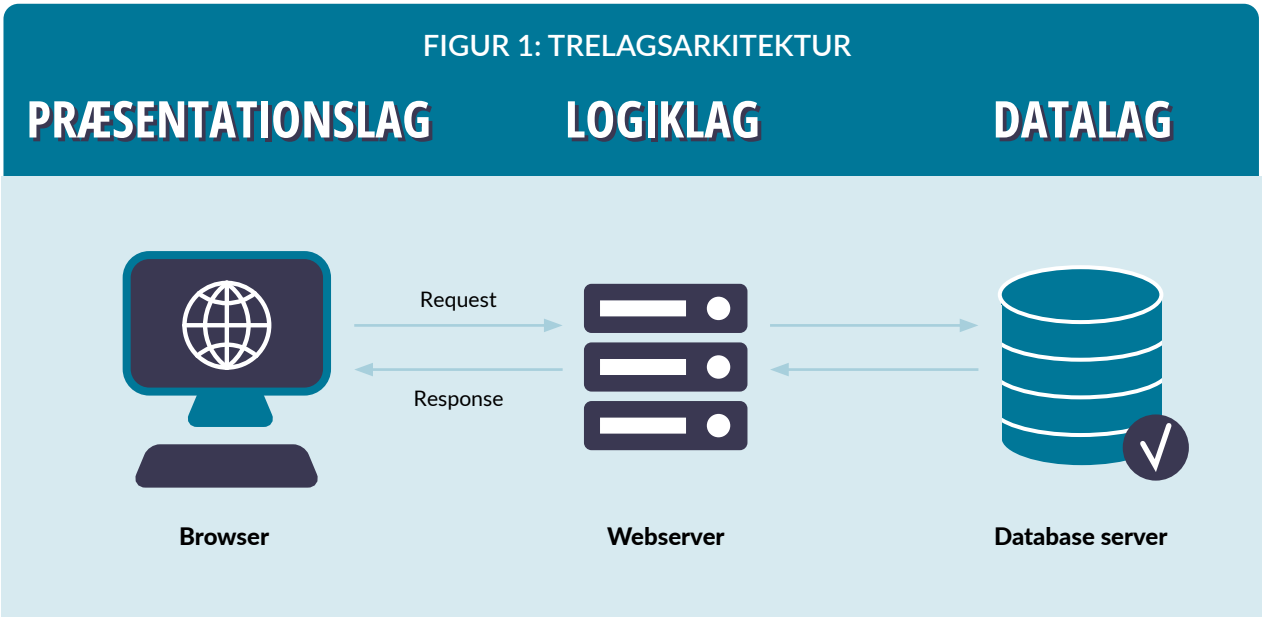
For at I kan arbejde med opgaverne i trin 1-3 skal I vide noget om trelagsarkitektur og om Haaukinsplatformen. Det er beskrevet herunder.

TRELAGSARKITEKTUR

Mange systemer, eksempelvis hjemmesider, består af en trelagsarkitektur: Et præsentationslag, et logiklag og et datalag. Se Figur 1.
Præsentationslaget er den pæne brugerflade med billeder, tekst, grafik osv. som brugeren navigerer i. Det er også her, man eventuelt logger ind på en hjemmeside. Logiklaget modtager information fra præsentationslaget, det kan være indtastninger, klik mm. Afhængig af, hvad kommandoerne er, kan der i logiklaget laves nogle beregninger eller sendes/hentes data fra datalaget. I datalaget opbevares data, man kan søge på data, og data kan sendes til logiklaget.

Hacking kan ske i alle lag. I de opgaver, I møder i denne mission, er der forskel på, hvor svaghederne skal findes. Du skal derfor forvente både at kigge på kode i logiklaget og data fra datalaget.

FIGUR 1: TRELAGSARKITEKTUR



HAAUKINSPLATFORMEN

Haaukins er en virtuel læringsplatform, hvor alle med interesse i cybersikkerhed kan træne og forstå 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.

Haaukins anvender Kali Linux som operativsystem og for at tilgå opgaverne skal man kende lidt til forskellige Linuxkommandoer, der kan være relevante at bruge i opgaverne. Når I arbejder med trin 0 lærer I om operativsystemet Linux og det virtuelle miljø, som Haaukins består af.

FORSKELLIGE TYPER AF HACKERANGREB

De challenges som I arbejder med i denne mission, beskriver forskellige typer af cybersikkerhedsangreb. Herunder kan I læse om angrebene og de forskellige challenges.

I opgaven *cookiesession* leder I efter en mulighed for at logge ind på en hjemmeside med en andens login og password. En af mulighederne er at kikke i cookies. En cookie er et stykke data, som man som bruger på en hjemmeside har med sig og giver til hjemmesiden automatisk. Den kan indeholde diverse informationer om brugeren, som hjemmesiden for eksempel bruger til at give selve brugeren adgang deres profil.

I opgaven *adminlogin* leder I efter en mulighed for at logge ind som administrator på hjemmesiden. Der er forskellige muligheder for det, som for eksempel at prøve sig frem og se, om der er en cookie, som indeholder den nødvendige information.
Både cookiesession og adminlogin illustrerer nogle af de problemer, mange brugere har, når password og login information ikke er sikret godt nok.

Opgaven Cross site request forgery er et eksempel på et cybersikkerhedsangreb med samme navn. Her opretter den cyberkriminelle et websted, som på grund af en svaghed i nogle websider, kan knyttes til en "rigtig" hjemmeside, som alle bruger. Det kan eksempelvis være en hjemmeside, som bruges i en fodboldklub eller en bank. Når den cyberkriminelle har udført sit angreb, kan han/hun eksempelvis tvinge brugeren til at skifte password, som så kan opfanges af den cyberkriminelle. Således kan den cyberkriminelle få adgang til hjemmesiden og begå kriminalitet.

I *FTP server login* kan man se, hvor nemt det er at gætte sig til et password. Dette angreb kaldes "brute force", fordi man bare prøver og prøver indtil man det lykkes.

JERES PRODUKT

For at gennemføre missionen, skal I forberede en præsentation, hvor I redegør for hvordan I har løst opgaverne og samtidig fremlægger jeres tre forslag til, hvordan I ville forhindre ondsindede hackere I at gøre det samme som jer. I præsentationen skal I:

- Redegøre for jeres mission
- Fortælle, hvordan I kom frem til jeres endelige løsningsforslag
- Præsentere jeres løsninger (gerne med billeder, video, skærmoptagelse mm)
- Komme med eksempler på, hvordan I kan overføre den viden, I har fået i opgaverne, til andre systemer/ sårbarheder
- 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 ind 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 upload-funktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.

"VÆR OPMÆRKSOM PÅ, AT HACKING KAN SKE I ALLE TRE LAG AF SYSTEMARKITEKTUREN."

TIL UNDERVISEREN, SOM ØNSKER AT ARBEJDE MED MISSION 3

BAGGRUND

I denne cybermission, skal eleverne arbejde i et virtuel cybertræningsmiljø, som hedder Haaukins. Her kan eleverne tilgå hjemmesider og elementer i IT-systemers trelagsarkitektur i et lukket virtuelt miljø. Så længe eleverne bliver i Haaukinsmiljøet og anvender den browser, der er i det virtuelle miljø, så sker der ikke noget, og eleverne kan udføre etisk hacking uden at være nervøse for at overtræde lovgivningen.

For at få adgang til de forskellige challenges, skal i skrive en mail til Mikkel Høst Christiansen på: mhch@es.aau.dk

Denne mail skal indeholde:

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

Mikkel vil herefter sende jer det link som eleverne skal oprette sig som brugere på.
HVIS der er problemer med challenges eller Haaukins, kan I til hver en tid kontakte Mikkel.

Såfremt eleverne ikke selv kan finde en oversigt over Linux-kommandoer, kan denne hjemmeside bruges: https://cheatography.com/davechild/cheat-sheets/linux-command-line/

FIND ALLE LØSNINGERNE PÅ PRAXIS ONLINE

Alle løsninger til challenges, som er nævnt i missionen, findes på Praxis Online https://online.praxis.dk/cyberskills i forløbet "Tænk som en hacker". For at tilgå løsningerne skal man først oprette sig som bruger, men det er helt gratis.

Vi vil bede om at elevernes løsninger ikke omdeles, da vi gerne vil have at andre skal kunne løse opgaverne uden at der ligger løsninger på Facebook, Discord eller andre steder.

OM DE FORSKELLIGE CHALLENGES

Cookie factory og *admin login* handler om cookies. Cookies er grundlæggende linjer af kode, der fortæller noget om, hvordan hjemmesider virker. De er nødvendige for navigation mellem faner i hjemmesider og kan indeholde tekniske beskrivelser samt information om koder, data om login-oplysninger mm.. De er således essentielle for den brugeroplevelse man har når man anvender hjemmesider. Der findes også cookies, der sikrer at der deles information mellem en hjemmeside og en tredjepart. De cookies handler mere om udbyderen end om brugeren. Det er således programmøren af hjemmesiden, der bestemmer, hvad der gemmes i cookies, og sikrer at de ikke kan læses af alle og enhver. Læs eventuelt mere om cookies på erhvervsstyrelsens hjemmeside her: https://erhvervsstyrelsen.dk/vaerd-at-vide-om-cookies

Den challenge, der er knyttet til *cross site request forgery* handler igen om, hvordan hjemmesiden er sat op af programmøren. Her skal man undersøge, hvad for noget data, der overføres af mellem hjemmesiden og den server den ligger på. Overførslen af data kan ske krypteret (https) eller ukrypteret (http). På linket her kan du læse, hvornår det er nødvendigt at anvende enten http eller https: https://www.alphaweb.dk/hvad-er-https/

Den challende, der hedder *FTP server login* sætter fokus på, hvor vigtigt det er at lave gode og lange passwords, som ikke umiddelbart kan gættes. Opgaven kan blandt andet åbne op for at snakke om kompleksitet og længde af passwords mm. På linket her, kan du læse hvad Center for Cybersikkerhed skriver om passwordsikkerhed: https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-vejledning-passwordsikkerhed-2020.pdf

LINKS TIL EKSTRAMATERIALE

Hvis eleverne skal have en mere udførlig introduktion til etisk hacking kan følgende eksempler være brugbare:

- I denne artikel fra Computerworld, fortæller Lene, som er certificeret hacker, om hvordan hun mener, at virksomheder er nødt til at kunne forstå, hvordan de gode hackere arbejder, for at kunne sikre sig selv: https://www.computerworld.dk/art/240352/lone-er-certificeret-hacker-hvis-man-vil-have-god-it-sikkerhed-er-man-noedt-til-at-forstaa-hvordan-de-gode-hackere-arbejder

- I denne artikel fra ITWatch, kan eleverne møde Henrik, som lever af at finde huller og hacke virksomheders IT-systemer: https://itwatch.dk/ITNyt/Brancher/arbejdsmarked/article11090603.ece

Forbrugerrådet TÆNK har i denne artikel samlet nogle simple råd, til at undgå hacking: https://taenk.dk/forbrugerliv/elektronik-og-digitale-tjenester/undgaa-hacking-saadan-goer-du-din-computer-sikker

På Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/ kan du finde en digital version af dette kompendium. Heri er alle links og henvisninger til digitale ressourcer klikbare.

MISSION 4 – GØR DET MULIGT AT VÆRE EN GOD HACKER

I Denne mission skal I lære, hvordan virksomheder kan skabe de rette rammer for etisk hacking og dermed bidrage til at styrke deres egen IT-sikkerhed.

I skal sætte jer i et firmas sted og hjælpe dem med at lave det, der kaldes et Vulnerability Disclosure Program. Skulle man oversætte begrebet til dansk ville det være noget i retningen af et "Sårbarheds Offentliggørelses Program". I praksis er det dog altid den engelske betegnelse, der bruges og det gør vi også i denne mission.

Et Vulnerability Disclosure Program (VDP) har til formål at give etiske hackere, også kaldet white hat-hackere, klare retningslinjer for, hvordan de indberetter potentielt ukendte og skadelige sårbarheder til de organisationer, der står bag systemet, så de kan blive fixet, til alles bedste.

Hvis ikke der findes et VDP for et system, kan etiske hackere risikere, uforvarende, at komme til at gøre noget ulovligt. Læs for eksempel denne artikel på dr om forælderen Esben, der fandt en sårbarhed i børnehavernes pladsanvisningssystem: https://www.dr.dk/nyheder/penge/it-gigant-anmeldte-esben-hacking-nu-dropper-politiet-sagen

Esben blev meldt til politiet for at hacke, selvom hans intentioner var gode. Hvis sagen var gået videre, kunne Esben have fået alvorlige problemer med loven.

Der var i dette tilfælde brug for at ejeren af systemet havde haft en VDP, så Esben trygt kunne indberette sin viden om den givne sårbarhed – uden at være bange for at ende i fedtefadet.

JERES MISSION

I denne mission skal I se på, hvordan man håndterer hacking i det virkelige liv. I skal forestille jer, at I er blevet hyret af sikkerhedsafdelingen i et stort softwareselskab. I har fået til opgave, at lave et udkast til et Vulnerability Disclosure Program (VDP), da virksomheden ønsker at etiske hackere kan hjælpe med, lovligt, at finde og afsløre sårbarheder i virksomhedens systemer.

I skal vælge hvilket softwareselskab I gerne vil repræsentere – det kan enten være:

1. Det nye system for digital identitet/digital post
2. Et socialt netværk
3. Et videospil

Inden I går i gang med jeres VDP, så læs den følgende sektion for at forstå, hvorfor hacking er blevet et samfundsmæssigt fænomen, og hvordan I kan lave en VDP for det softwareselskab, I har valgt.

HACKING SOM ET SAMFUNDSMÆSSIGT FÆNOMEN

Der opstår hele tiden sårbarheder i software på grund af nye opdateringer, manglende opdateringer, nye funktionaliteter, uhensigtsmæssig brug af software m.m. Hackere har en stor interesse i at udnytte disse sårbarheder for at kunne lave et angreb.

Hacking er et stort samfundsmæssigt problem, hvor virksomheder, offentlige myndigheder og privatpersoner taber milliarder af kroner til hackere. Det kan eksempelvis være igennem virus, ransomwareangreb, phishing.

Hvis vi som samfund skal have en chance for at beskytte os mod hackerangreb, så er det vigtigt, at vi opnår samme faglige niveau som dem, der angriber os.

Vi skal derfor skabe gode rammer for at etiske hackere kan hjælpe med at lukke sårbarheder, fx med det formål at beskytte samfundet, uden at risikere at blive sagsøgt for det og ende i fedtefadet hos politiet.

Som inspiration til at løse jeres mission kan I fx. høre denne episode af DR podcasten Genstart. Her fortæller Jacob, der er studerende og professionel hacker, om den cyberkriminelle gruppe The Dark Side, om sin egen historie som professionel hacker og om, hvordan han sørger for at holde sig på den rigtige side af loven.

Link til podcast – episoden tager 23 min.: https://www.dr.dk/lyd/special-radio/genstart/genstart-2021-05-25

Se videoen om VDP'er under videomateriale på Cybermissionens hjemmeside:
https://cybermissionen.cyberskills.dk/

HVAD ER EN GOD VDP?

En god VDP hjælper virksomhederne, fordi den motiverer etiske hackere til, at indrapportere de sårbarheder de finder – fordi de ved, at de kan gøre det på lovlig vis uden at havne på den forkerte side af loven.

Hvis ikke man har en god VDP, betyder det måske, at sårbarhederne ikke bliver indrapporteret eller endnu værre, at de bliver solgt på det sorte marked.

En VDP hjælper også med at vise, at virksomhederne er ansvarsbevidste i forhold til deres egen sikkerhed, og ofte vil brugernes tillid blive øget.

Der findes flere metoder til at lave en VDP. I denne mission anvender vi "A Framework for a Vulnerability Disclosure Program for Online Systems" fra det amerikanske Justitsministerium. I kan læse hele framworket i pfd'en her: https://www.justice.gov/criminal-ccips/page/file/983996/download

VDP'en skal tydeligt beskrive tilladt adfærd vedrørende opdagelse og offentliggørelse af sårbarheder, således at risikoen for strafbare overtrædelser af loven reduceres.

Processen med at udarbejde en VDP består af fire trin, som beskrives nedenfor. I kan lade jer inspirere af processen og følge anbefalingerne til, hvordan man som virksomhed udarbejder en god VDP.

DE FIRE TRIN I EN VDP

TRIN 1

LAV EN PLAN FOR OFFENTLIGGØRELSE AF SÅRBARHEDER

Ved udarbejdelsen af en VDP skal I hjælpe virksomheden med at beslutte, hvilke aktiver, altså det der har værdi for virksomheden, der skal medtages i planen. Skal det være alle aktiver eller udvalgte?

Denne beslutning kan være påvirket af flere faktorer, herunder om det undersøgte system behandler følsomme oplysninger, om nogle sikkerhedsforanstaltninger allerede er på plads, virksomhedens evne til at opdele netværket, lovgivningsmæssige og kontraktlige forpligtelser osv.

Virksomheden bør afgøre, om VDP'en skal skelne mellem typer af sårbarheder, fx softwarefejl, dårlig adgangskodestyring, fejlkonfigurerede systemer, social engineering.

TRIN 2

PLAN FOR ADMINISTRATION AF VDP

I trin 2 skal I beslutte, hvordan sårbarheder skal rapporteres. Først og fremmest hvilken e-mailkonto inde i virksomheden, de etiske hackere skal kontakte. Det skal helst være en mailadresse med et alias i stedet for en personlig konto, for eksempel security@example.org.

Desuden bør I beslutte, hvordan sårbarhederne skal indberettes. Hvilke oplysninger skal der gives? Hvad er rapportens forventede kvalitet? Skal der fremlægges et proof of concept, som viser, hvordan man udnytter sårbarheden?

Sammen med oplysninger om selve rapporten skal I angive tidsrammen for rapportering. Skal det ske ved opdagelse, eller når sårbarheden er fuldt valideret?

Endelig bør I beslutte, hvordan I ønsker at håndtere overtrædelser af VDP'en, både dem der er sket i god tro og bevidste overtrædelser i ond tro.

TRIN 3

LAV ET UDKAST TIL JERES VDP

Når I laver udkastet til jeres VDP-dokument, er det vigtigt, at I får beskrevet autoriseret og uautoriseret adfærd i enkle, letforståelige betingelser, så udefrakommende kan forstå det.

I skal derfor identificere netværkskomponenter eller data i den politik, der er inden for rammerne af planen, så specifikt som muligt. I skal beskrive, hvordan man identificerer oplysninger, der ikke er inden for rammerne af programmet.

Det er også vigtigt at forklare konsekvenserne af at overholde og ikke overholde politikken. Det er f.eks. nyttigt at overveje følgende formuleringer:

1. Organisationen vil ikke anlægge sag for utilsigtede overtrædelser af sin politik i god tro eller indlede en klage til retshåndhævelse for utilsigtede overtrædelser.
2. Organisationen anser aktiviteter, der udføres i overensstemmelse med politikken, for at udgøre "autoriseret" adfærd i henhold til loven om computerbedrageri og misbrug.
3. Hvis der anlægges sag af en tredjepart mod en part, der har overholdt politikken for afsløring af sårbarhed, vil organisationen tage skridt til at gøre det kendt, enten for offentligheden eller for retten, at personens handlinger blev udført i overensstemmelse med politikken.

Endelig skal I huske at nævne at etiske hackere skal kontakte organisationen for at få en afklaring, før de deltager i en adfærd, der kan være uforenelig med eller ikke er adresseret af politikken (VDP'en).

TRIN 4

IMPLEMENTÉR PLANEN OG SKAB KENDSKAB

Når I har et dokument, der klart beskriver jeres VDP, skal I hjælpe virksomheden med at gøre det bredt tilgængeligt. Der kan for eksempel linkes til den direkte på virksomhedens hjemmeside. Det anbefales også at reklamere for VDP´en på passende steder. Det skal I også hjælpe virksomheden med. Hvordan vil I kommunikere og gøre jeres VDP tilgængelig for relevante parter?

Et brugbart sted at reklamere for virksomhedens VDP er de såkaldte URI'er eller "well-known URIs". Velkendte URI'er er en standardplacering på et websted for at gemme brugbare oplysninger om virksomhedens sikkerhedspolitik. Hvis virksomhedens hjemmeside er www.example.com, kunne det eksempelvis være på følgende URL at man gemte sin VDP: https://www.example.com/.well-known/security.txt.

INSPIRATION FRA ANDRE VDP'ER

Når I udarbejder virksomhedens VDP, kan I lade jer inspirere af de allerede eksisterende politikker om vulnerability disclosure. I kan google jer frem til en del på hjemmesiderne HackerOne eller BugCrowd.

I kan starte med at kigge på Dropbox vulnerability disclosure document på linket her: https://hackerone.com/dropbox

JERES PRODUKT

Det er op til jer, hvordan I udformer virksomhedens VDP. Det kan være et skriftligt produkt, en slide-præsentation, en video-præsentation eller noget helt andet.
Forsøg at følge de fire trin så godt som I kan. I må meget gerne inkludere jeres argumenter for, hvordan I er nået frem til den givne VDP.

JERES PRÆSENTATION

I skal forberede en præsentation af jeres VDP, hvor I redegør for missionen og fortæller om jeres proces med at udarbejde VDP'en. I præsentationen skal I:

- Redegøre for jeres mission og den virksomhed, I har valgt at arbejde for
- Præsentere jeres VDP (gerne med billeder, video, skærmoptagelse m.m.)
- Fortælle, hvordan I har anvendt alle eller dele af de fire trin til at lave jeres VDP
- Argumentere for, hvilken effekt I tror, at jeres løsning kan få hos jeres virksomhed
- 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 ind 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.

"EN VDP GIVER ETISKE HACKERE RAMMER FOR AT HJÆLPE VIRKSOMHEDER MED AT FORBEDRE DERES IT-SIKKERHED."

MISSION 5 – (U)SIKKERHED I SMART HOME ASSISTANTS

Smart home assistants som for eksempel Amazon Alexa, Google Assistant eller Appels Siri bliver mere og mere udbredte i hjemmene hver eneste dag. Måske er det også almindeligt for din familie at have sådan en i jeres hjem?

Disse devices lytter til stemmekommandoer og reagerer på dem ved at bruge deres internetforbindelse.

Men vi tænker måske ikke over, at det åbner for nogle sikkerhedsproblemer, når en smart home assistant får en kommando, henter data fra nettet, giver besked til brugere om opkald/beskeder, eller bruges til at kontrollere andre IOT-devices i hjemmet.

I er nu kommet på en mission for at gøre jeres hjem mere sikre ved, at begrænse truslerne mod smart home assistants. Med udgangspunkt i to modeller (dataflow diagram og STRIDE som præsenteres senere) skal I undersøge, hvordan man identificerer sårbarheder i systemerne og derved måden, hvorpå de kan hackes. Ved at identificere sårbarhederne, vil I også være i stand til at komme med forslag til, hvordan sikkerheden i systemerne kan øges.

JERES MISSION

I skal lave en trusselsmodellering af en smart home assistant. Det kan virke som en stor opgave.
Vi har derfor brudt trusselsmodelleringen lidt op, for at gøre det lettere for jer.

For at løse jeres mission skal I besvare de følgende 5 trin, som samlet set udgør jeres trusselsmodellering.

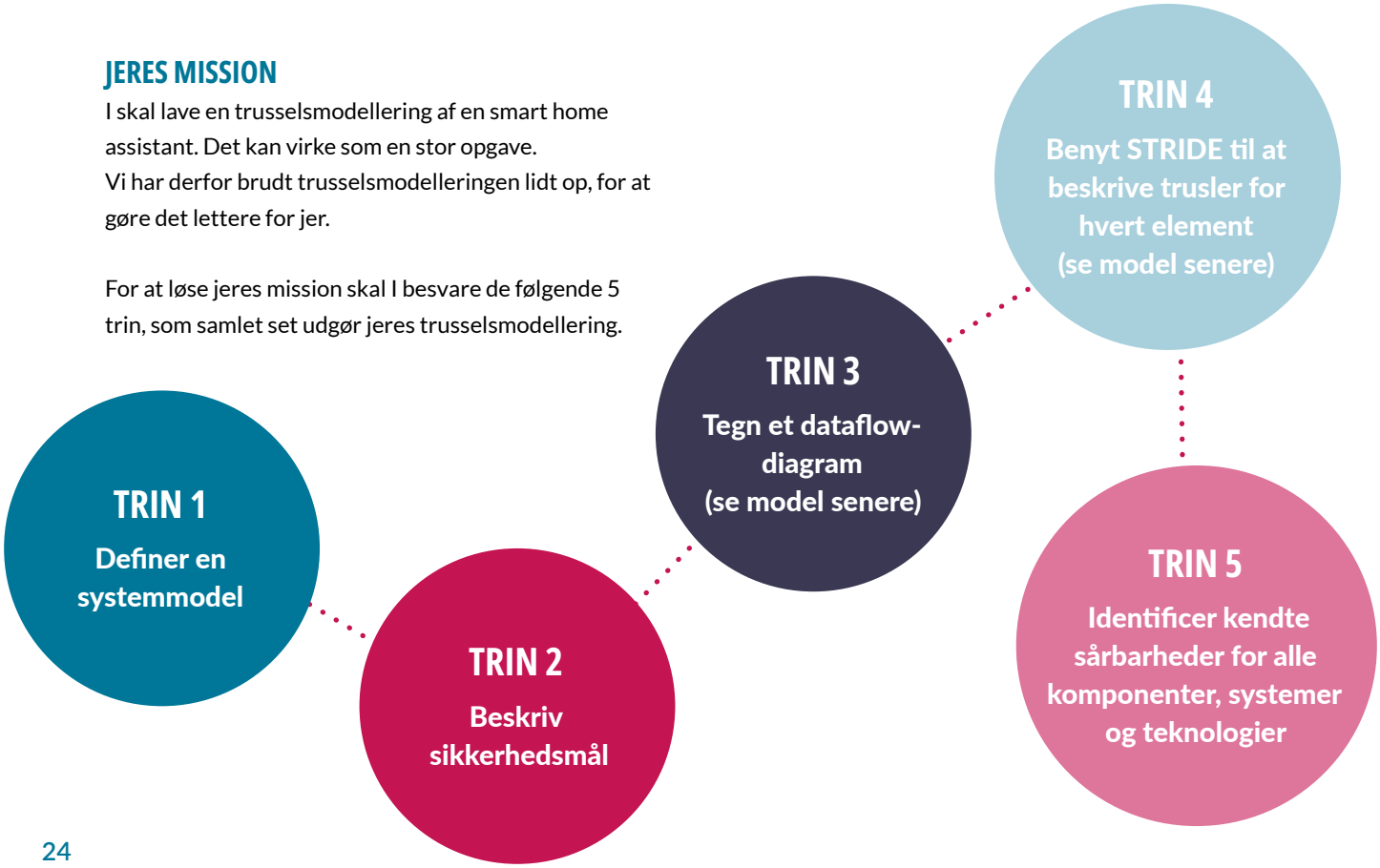
Vi anbefaler, at I udarbejder et STRIDE-framework og et dataflow-diagram til at understøtte jeres besvarelse. De to modeller er beskrevet til sidst i missionen.

BAGGRUND: HVAD ER EN 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.

Formålene med en trusselsmodellering er at:

- Forstå de sikkerhedsmål, man søger at realisere
- Forstå det system, man forsøger at sikre
- Forstå de trusselsaktører, man står overfor
- Forstå de teknikker, trusselsaktørerne benytter (angrebsvektorer)
- Forstå de sårbarheder, angriberne udnytter
- Forstå, hvilke modforholdsregler, der er effektive mod disse angreb



VIGTIGE HOVEDTERMER INDEN FOR TRUSSELS-MODELLERING, SOM ER GODE AT KENDE

Trussel. En trussel er en potentiel uønsket begivenhed eller hændelse, der kan skade eller kompromittere et aktiv eller mål. Den kan være af ondsindet natur.

Angreb (eller udnyttelse). Et angreb er en handling, der udnytter en eller flere sårbarheder for at gennemføre en trussel.

Sårbarhed. En sårbarhed er en svaghed, som muliggør et angreb, i en del af et system. Sårbarheder kan findes i niveauet for netværk, host eller applikation og inkluderer operationelle praksisser.

Modforholdsregler. En modforholdsregel tager fat på en sårbarhed for at reducere muligheden for angreb eller reducere et angrebs påvirkning. En modforholds-regel forholder sig ikke direkte til en trussel. I stedet tager den fat på de faktorer, der definerer truslen. Modforholdsregler spænder fra at forbedre en applikations design eller kode til at forbedre en operationel praksis.

Aktiv. Et aktiv er en ressource, der har værdi. Det varierer efter perspektiv. For en virksomhed kan et aktiv være informationer såsom kundedata. Eller det kan være mere uhåndgribeligt, som fx virksomhedens omdømme. Det kan også være muligheden for at misbruge virksomhedens applikation til at få uautoriseret adgang til data, administrative funktioner eller lignende.

SÅDAN LAVER DU EN TRUSSELSMODELLERING TRIN FOR TRIN

Der er fem trin i en trusselsmodellering, som du kan se uddybet i det følgende.

TRIN 1

DEFINER EN SYSTEMMODEL

- Identificer jeres smart home assistentens' system-komponenter og interaktioner mellem dem. Hvad kan systemet, hvem bruger det og hvordan?

TRIN 2

BESKRIV SIKKERHEDSMÅL

- Beskriv de overordnede sikkerhedsmål for systemet som helhed
- Beskriv sikkerhedsmålet for de enkelte komponenter, som systemet består af

TRIN 3

TEGN ET DATAFLOW-DIAGRAM (SE MODEL 1)

Dataflow-diagrammet beskriver, hvordan data bevæger sig gennem et netværk.

- Tegn et diagram, der beskriver alle datastrømme i jeres smart home assistent.

TRIN 4

BENYT STRIDE TIL AT BESKRIVE TRUSLER FOR HVERT ELEMENT (SE MODEL 2)

- Trusselsvurderingen bør indeholde en linje for hvert element (dvs. systemkomponent) som I identificerede i trin 1.
- For alle krydser bør der være en beskrivelse af den specifikke trussel
  - Fx hvorfor er spoofing et problem for bluetooth-parring i en Soundboks? Se en mere detaljeret beskrivelse af STRIDE-modellen nedenfor.

TRIN 5

IDENTIFICER KENDTE SÅRBARHEDER FOR ALLE KOMPONENTER, SYSTEMER OG TEKNOLOGIER

- Analysér systemet for sårbarheder der kan udnyttes.

SÅDAN LAVER DU ET DATAFLOW-DIAGRAM

Det kan være godt at spørge sig selv, hvad der sker med data, når de kommer til et system. Om de omregnes eller konverteres på en eller anden måde, om de gemmes i en database og, hvordan data sendes videre til et nyt system eller til et andet sted i systemet.

Et dataflow-diagram viser, hvordan data strømmer igennem et system eller igennem en række af forskellige systemer. Det bruges ofte i softwareudvikling til at give et overblik over, hvor data er, hvornår og med hvilket formål.

Dataflow-diagrammet viser blandt andet, hvor data kommer fra, hvor de går hen, hvor de bliver gemt og hvor de måske transformeres, eksempelvis fra stemme til skrift. Følgende symboler kan bruges i diagrammet:

MODEL 1: SYMBOLER TIL DATAFLOW-DIAGRAM

TEKST →	En pil angiver den retning, som data bliver sendt i
PROCES	En cirkel (eller oval) angiver, hvor data processeres eller transformeres
KILDE	En firkant angiver, at data sendes til en ekstern kilde (i forhold til hvor data startede)
DATA	To streger med tekst imellem angiver, hvor data gemmes (i en database eller lignende)

Man kan starte med et overordnet billede af, hvad der sker med data for at forstå nogle af de eksterne kilder. Derefter kan man dykke et skridt dybere for at forstå, hvad der sker på et detaljeret niveau.

Under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/ finder I en video, som viser, hvordan man kan lave et dataflow-diagram.

SÅDAN LAVER DU EN STRIDE-MODEL

STRIDE-modellen er et nyttigt værktøj, som kan hjælpe med at klassificere trusler. Modellen er oprindeligt udviklet for at hjælpe sikkerhedsingeniører.

HVAD STÅR STRIDE FOR?

STRIDE er et akronym for seks trusselskategorier:

- **Spoofing**: agenter udgiver sig for at være en anden
- **Tampering**: uautoriserede ændringer af systemer eller data
- **Repudiation**: agenter nægter at have sendt en besked eller udført en handling
- **Information leakage**: fortrolighed brydes, fordi information lækkes til udenforstående
- **Denial of Service (DoS)**: systemer eller data gøres utilgængelige for autoriserede brugere
- **Elevation of Privilege**: agenter opnår højere privilegier, f.eks. administratorrettigheder

Her er et eksempel på, hvordan man bruger STRIDE:

STRIDE tager udgangspunkt i de elementer, man har identificeret i dataflow-diagrammet. Vi har indsat følgende element " #1 Parring mellem telefon og Soundboks" i STRIDE-modellen nedenfor.

MODEL 2: STRIDE

	ELEMENT	INTERACTION	S	T	R	I	D	E
1	BT forbindelse	Parring mellem telefon og Soundbox	X				X	
2		Afspilning af musik	X	X			X	
3		Kontrol af Solundbox (tænd/sluk, volumen, ...)	X	X			X	X
4								

Under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/ finder I en video, som gennemgår STRIDE-modellen.

S: Spoofing kan tillade at uautoriserede telefoner parres med Soundboks eller at en telefon parres med uautoriseret Soundboks.

D: Spoofing tillader direkte DoS ved at slukke for boksen, skrue ned for lyden, spille noget helt andet eller afbryde parring.

Lav jeres eget STRIDE skema og start med at indsætte de elementer i identificerede i trin 1. Herefter kan I bruge modellen til, at hjælpe med at skabe et overblik over trusler og dermed også eventuelle sårbarheder jeres system måtte have.

Når I har lavet alle punkterne i trusselsmodelleringen har I gennemført missionen.

JERES PRÆSENTATION

I skal forberede en præsentation af jeres analyse, hvor I redegør for missionen, fortæller om jeres proces med at lave jeres trusselsmodellering samt præsentere selve trusselsmodelleringen. I præsentationen skal I:

- Redegøre for jeres mission og hvad I har valgt at fokusere på
- Fortælle, hvordan I kom frem til jeres endelige trusselsmodellering
- Præsentere jeres modellering (gerne med billeder, video, skærmoptagelse m.m.)
- Fortælle, hvordan I har anvendt modeller/analyseredskaber
- Præsentationen skal have karakter af et 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 ind 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.

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

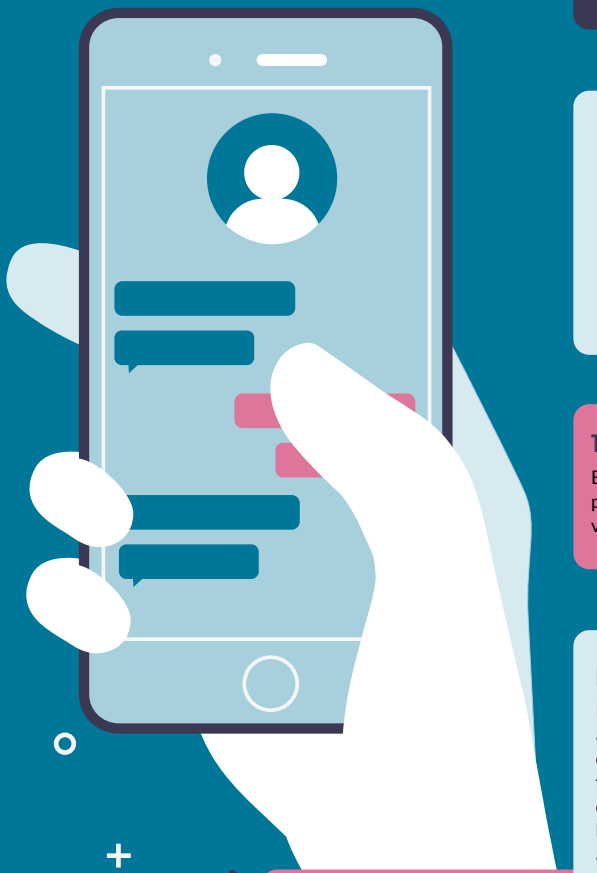
Mange virksomheder laver cyber awareness træning. Det kan eksempelvis være kommunikationsaktiviteter eller uddannelse, der skaber opmærksomhed om informationssikkerhed hos medarbejderne, så de får en mere sikker digital adfærd.

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.

Kan I finde flere ord?

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING

CYBER SKILLS

CYBERMISSIONEN - NOTER

CYBERMISSIONEN - NOTER

CYBERMISSIONEN - NOTER

CYBERMISSIONEN

BØRNE- OG
UNDERVISNINGSMINISTERIET
STYRELSEN
FOR IT OG LÆRING

CYBER SKILLS