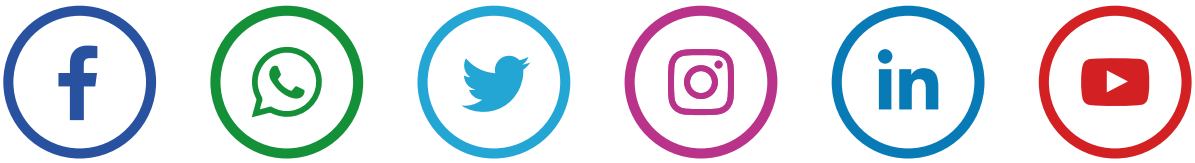
MISSION 5: DEL OG HERSK! STYR DINE DATA!



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