MISSION 5: Hjælp virksomheden SneakPeak med at undgå hacking

Velkommen til cybermissionen!

I denne mission skal I hjælpe virksomheden **SneakPeak** med at styrke deres fokus på cybersikkerhed!

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. På det seneste har virksomheden modtaget en del falske mails og opkald. SneakPeaks ejer Line vil gerne have, at hendes medarbejdere bliver klogere på cybersikkerhed, og derved også bliver bedre til at spotte og undgå forsøg på cyberangreb på virksomheden. Med indtoget af kunstig intelligens er emnet kun blevet endnu mere relevant, fordi generativ AI som fx ChatGPT også er et godt værktøj for hackere til at lave endnu bedre angreb.

I denne mission skal I hjælpe Line og hendes medarbejdere med at blive klogere på cybersikkerhed og komme med eksempler på, hvad de skal være opmærksomme på. Det skal I præsentere for dem i slutningen af missionen.

Men først skal I selv blive lidt klogere på generativ AI og cybersikkerhed.

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. Nu havde vi et navn, men manglede et logo. Vi brugte et andet AI-værktøj, som kun kan lave billeder, til at hjælpe os med den del – 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. Det samme gælder for hackerne.

Hvad er generativ AI?

Inden vi dykker ned i generativ AI, skal vi først lige have styr på, hvad AI dækker over. AI står for "Artificial Intelligence", som på dansk hedder kunstig intelligens. Emilie Lundblad, tidligere Managing Director hos Amesto Nextbridge, arbejder med data og kunstig intelligens, og ved derfor rigtig meget om teknologien. I videoen herunder giver Emilie dig en kort introduktion til, hvad kunstig intelligens handler om.

Video: Hvad er kunstig intelligens
https://cybermissionen.cyberskills.dk/videomateriale2024/

Kunstig intelligens kan både være mere simple ting, som når du låser din mobil op ved hjælp af ansigtsgenkendelse, stavekontrol når du skriver beskeder, 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 Skjærven, der er stifter af Future Scouts og har arbejdet med teknologi i mere end 20 år, vil nu, i videoen, fortælle dig om, hvad generativ AI er.

Video: Hvad er generativ AI?
https://cybermissionen.cyberskills.dk/videomateriale2024/

Du har måske allerede gjort dig erfaringer med et generativ AI-værktøj, fx ChatGPT. ChatGPT hører ind under betegnelsen generativ AI, da du kan få værktøjet til at skabe ny, unik tekst til dig. Der er også andre AI-værktøjer, der kan skabe billeder, videoer eller musik.

Hvad er cybersikkerhed?

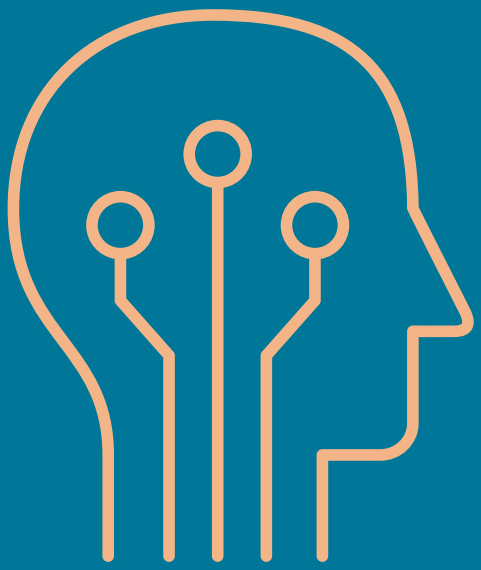
Cybersikkerhed handler om at undgå at hackere kan snyde os

Der findes overordnet to måder, som hackere forsøger at snyde dig på. Den ene er ved at fiske oplysninger fra dig, som du afgiver i god tro - det kan være via e-mail eller telefon. Den anden er via malware eller ransomware, der er en lille, ondsindet software, som de inficerer din computer med, og derved enten stjæler oplysninger eller låser virksomhedens data fast fx med det formål efterfølgende at opkræve virksomheden betaling for at frigive data igen. For at mindske risikoen for at blive snydt, har SneakPeak brug for at få klarhed over, hvilke måder de kan blive angrebet på.

Hvad er hacking?

Politiet forklarer hacking på følgende måde:
"Hacking er, når nogen uden din tilladelse skaffer sig adgang til din computer, dine programmer, din e-mail eller din konto på sociale medier. Hacking kan fx indebære, at der er nogen, der sletter, ændrer eller kopierer dine oplysninger."

https://politi.dk/anmeld-kriminalitet/hacking/anmeld-hacking



"Machine Learning" eller maskinlæring på dansk er, når mennesker lærer en maskine at gøre noget, som ellers vil kræve, at et menneske gjorde det.

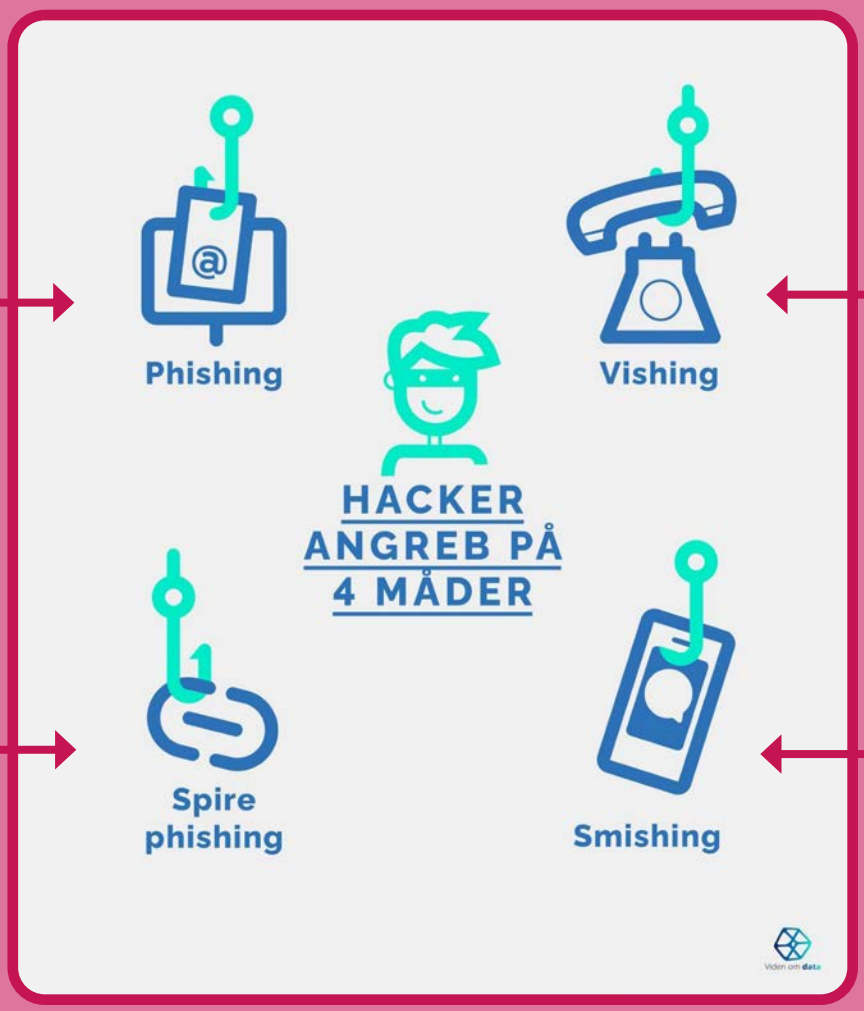
Maskinen bliver trænet til at genkende mønstre, og kan på den baggrund bruges til fx at foreslå varer på en webshop eller finde phishing mails i din mailboks.

Phishing

Her forsøger hackerne at fiske oplysninger ved at bede dig sende oplysninger til dem via e-mail.

Vishing

Står for Voice phishing. Her ringer en hacker til den person, som de gerne vil have til at gøre noget bestemt, fx ændre et kontonummer eller afgive bestemte oplysninger.



Spire phishing

Her målrettes et phishing angreb direkte mod én bestemt person i virksomheden, som hackeren mener at vide, med stor sandsynlighed vil åbne linket eller reagere på deres snyd. Fænomenet breder sig mere og mere.

Smishing

Ordet smishing er en sammensætning af "sms" (short message services) og "phishing". Ved smishing sker det samme som phishing, men gerningsmanden bruger SMS i stedet for e-mail.

Det vigtigste SneakPeak kan gøre, er altså at forholde sig kritik, hvis de modtager links, eller bliver bedt om at udlevere oplysninger. Derudover er det vigtigt, at vide, hvad man skal gøre, hvis man bliver hacket. Det fortæller Tina Hentze, som er Department Manager i afdelingen Business Infrastructure & Security hos kaastrup|andersen, om i podcasten her:

Podcast: Viden om data (soundcloud.com)
03 Hvis man som medarbejder kommer til at udfordre sikkerheden, hvad gør man så?: https://cybermissionen.cyberskills.dk/videomateriale2024/

Hackere er rigtig dygtige til at få adgang til virksomheders data, og nogle hackergrupper har mange kræfter, de sætter ind på at få adgang til virksomheders forskellige enheder som computer, telefon og tablets osv. Derfor arbejder mange virksomheder også med et Red Flag og et Blue Flag hackerteam. Red Flag teamet har til opgave at angribe virksomheden på de svage punkter og dermed forsøge at finde hullerne. Blue Flag skal modsat forsøge at forsvare virksomheden mod angrebene og også prøve at regne hullerne ud, så de kan forsvare og lukke dem. Det er dog kun store virksomheder, der har den type af muligheder. Den slags ressourcer har SneakPeak ikke, og derfor har de brug for din hjælp til at gennemskue, hvor hullerne kan være. Det kommer vi tilbage til om lidt.

Råd til at undgå hackere

Der findes en række råd, man som virksomhed og privatperson kan følge for at mindske risikoen for at blive hacket:

Opdatér:
Det er vigtigt, at du opdaterer din computer og telefon løbende, for at sikre at enheden har de nyeste sikkerhedsopdateringer. Ved at sikre at din enhed er opdateret, har du et bedre forsvar mod et potentielt angreb.

Backup:
Hvis virksomheden har backup af indholdet på telefoner og computere (fx billeder og dokumenter), taber virksomheden ikke noget ved, at hackerne låser deres data.

Password:
Du har helt sikkert hørt det før, men det er vigtigt at have et stærkt password. Simple koder kan hurtigt knækkes, og så kan hackeren potentielt have adgang ind i hele jeres virksomhed eller til al din personlige data. Husk også at skifte dem jævnligt.

Antivirus:
Antivirus programmer er en effektiv måde at mindske risikoen for at blive hacket på. Programmet scanner din enhed for at stoppe et angreb. Husk at opdatere programmet løbende.

Åbne netværk – pas på:
Åbne netværk kan være en hackers forfalskning af din lokale cafés netværk. Hvis du logger på det, kan det give hackeren adgang til dine eller din virksomheds data.

Undgå at betale:
Hvis virksomheden eller du selv er blevet udsat for et angreb, er det fristende at betale hackerne for at slippe data fri igen. Men hvis man gør det, er det sandsynligt, at man bliver ramt igen, da de nu ved, at man betaler. Det er heller ikke sikkert, at man får sine data, selvom man giver dem det, de efterspørger.

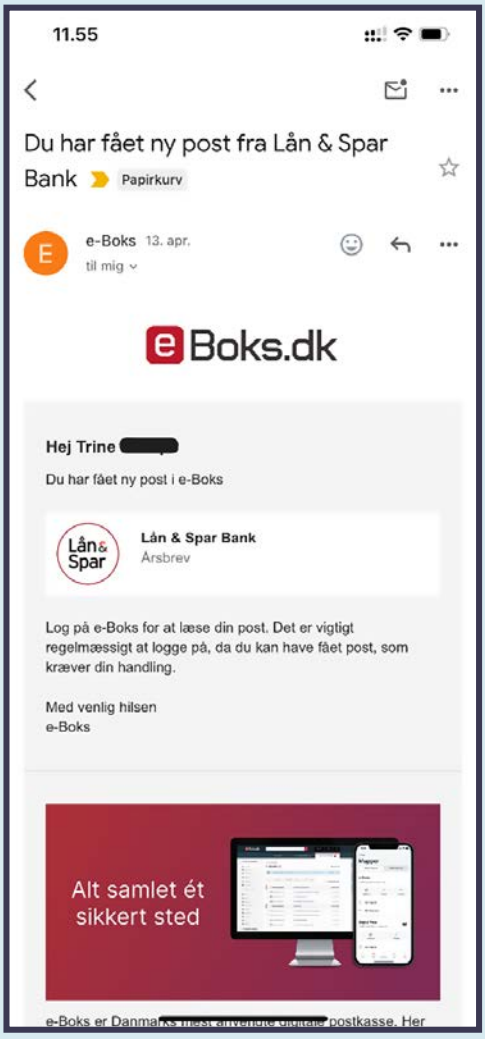
Se nedstående video hvor Tom Engly fra Tryg Erhverv fortæller om, hvad du som medarbejder kan gøre for at mindske risikoen for at blive hacket:

Video (Tryg Forsikring):. 8 gode råd til at forebygge cyberangreb.
https://tryg.dk/erhverv/rad-til-forebygge-cyberangreb

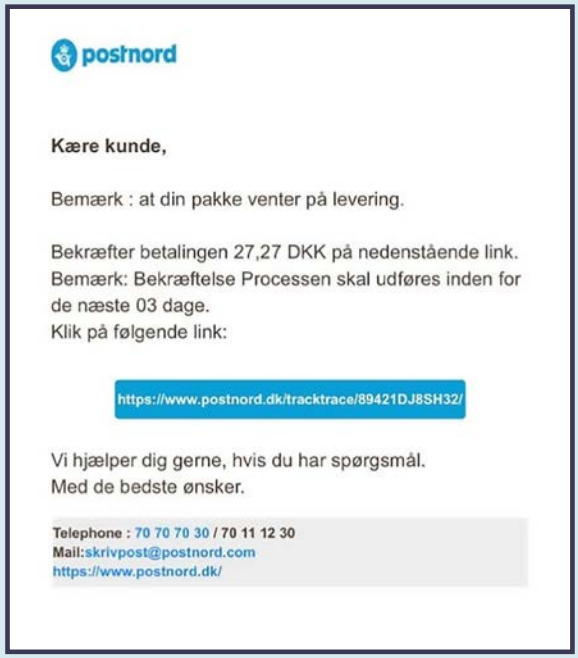
OPGAVE - Spot hackernes bullshit

Forsøg at udpege, hvilke af nedenstående e-mails og SMS'er, som er falske. Kun én er rigtig, mens tre er falske. **Begrund svarene**.

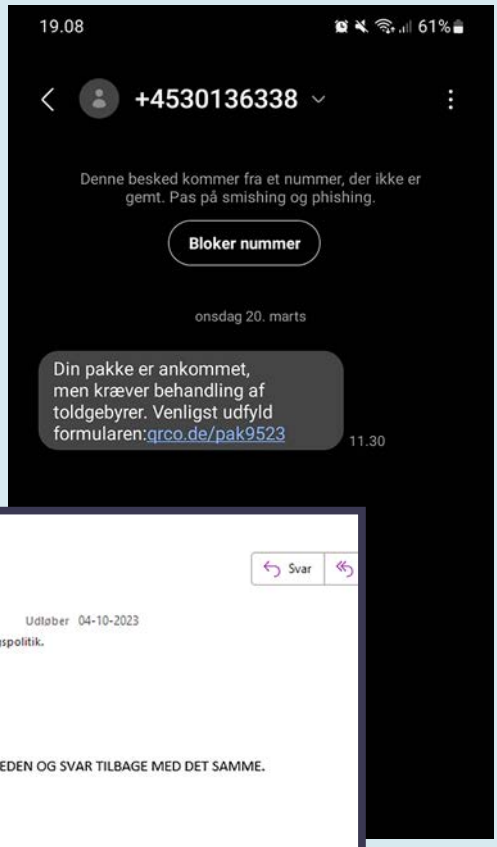
1



2



3



4

Sådan snyder hackere ansatte i virksomheder

Ifølge IBM er den mest udbredte måde for virksomheder at få stjålet data på gennem brugernavne og kodeord, som hackerne har fået adgang til. Denne type af angreb på virksomheder udgjorde i 2021 19% af alle læk. Det er også denne type af læk, som tager længst tid at identificere. I gennemsnit brugte virksomhederne 243 dage på at finde frem til lækket. Phishing kommer ind på andenpladsen over de mest udbredte metoder, som hackere bruger mod virksomheder, da 16% af angrebene bliver foretaget på denne måde.

IBM (2022) *Cost of a Data Breach*, Report 2022. Lokaliseret d. 10/9/2022 på:
https://www.ibm.com/downloads/cas/3R8N1DZJ

Generativ AI og hacking

Tidligere har vi sagt, at vi skal se det, før vi tror det. Den tid er endegyldigt forbi, fordi generativ AI giver helt nye muligheder for at skabe troværdigt indhold, som kan få medarbejdere til at udlevere oplysninger. Med generativ AI er det blandt andet blevet muligt for hackere at skabe videoer på baggrund af billeder af medarbejdere. Hackerne kan også foretage telefonopkald, hvor de fx bruger chefens stemme til at give en medarbejder en instruks om udlevering af oplysninger. Med generativ AI bliver det også lettere for hackerne at lave personaliserede, målrettede og troværdige mails og beskeder, som ser ægte ud, fordi den er god til at oversætte til forskellige sprog og skrive på en troværdig måde.

Du tænker måske, at det er helt vildt svært og kompliceret at skabe den slags videoer og lydbidder. Men her kan du se en video med Michael Andersen, Datagidselforhandler, der fortæller om, hvor let det kan gøres.

Video (youtube.com): cyberangreb med stemmekloning

https://www.youtube.com/watch?v=cH8mqs2djsQ

Overvej: Hvordan er det mest sandsynligt, at SneakPeak bliver hacket? Hvilke kanaler kan du forestille dig at en virksomhed som SneakPeak har, hvor hackere kan angribe sig igennem?

Afsluttende præsentation

i skal nu lave en præsentation til virksomheden SneakPeak. Tag udgangspunkt i de overvejelser, I har gjort jer gennem forløbet. Brug eventuelt grafikken med eksempler på angrebstyper i jeres præsentation.

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

- **Forklar generativ AI** og hvordan det kan bruges af hackere.
- **Kom med eksempler på**, hvordan SneakPeak kan angribes og forklar, hvad typerne af angreb går ud på.
- **Lad som om I er et Red Flag team**: Hvis I skulle angribe SneakPeak, hvad ville I så gøre?
- **Lad som om I er et Blue Flag team**: Hvad skal SneakPeak være opmærksomme på for at undgå potentielle angreb?

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.