



Cyber Awareness

(Virksomhedskultur,
kommunikation, strategi
forandringsledelse osv....)



**Hvorfor er awareness relevant, interessant
og spændende at arbejde med?**



Der var ikke tale om et bluff, da ransomwarekartellet LockBit for nylig truede med at lække Vestas' data.

Hackere har offentliggjort Vestas-data på nettet: Tusindvis af kunders finansielle oplysninger lækket

TEKNOLOGI

Var tæt på at slukke tusindvis af vindmøller: Nu fortæller Vestas om cyberangreb

Danmarks fjender står lige foran hoveddøren, siger amerikansk cyber-forfatter.

Kilde: DR

Hackerne går især efter de mindre virksomheder

El-installatørs filer krypteret

En el-installatør, der ikke kunne få adgang til sit økonomisystem, opdagede, at alle filer på drevet var blevet krypteret. Han blev kontaktet af hackere, der krævede en løsesum for at låse filerne op. Angrebet mistænkes for at være startet ved et forkert klik på et link.

Ved ekstern IT-rådgivning lykkedes det at genskabe al data, men regningen løb alligevel op i 55.400 kr.

Isenkræmmers webshop ramt af malware

En isenkræmmer opdagede, at hans hjemmeside var blevet ramt af malware, som gjorde, at et hacket betalingsvindue åbnede op i stedet for kundens eget.

Det lykkedes heldigvis ikke at få nogen kunder til at gennemføre betalinger i det nye betalingsvindue - men skadeudgiften for fjernelse af malware samt driftstab nåede at runde 82.000 kr.

Kilde: TopDanmark¹

Hackerne går især efter de mindre virksomheder

Tøjbutiks IT-system låst af hackere

En tøjbutik blev udsat for et hackerangreb, hvor en såkaldt cryptolock-virus blev installeret i virksomhedens IT-system. Det betød, at alle butikkens IT-systemer var låst og ikke kunne tilgås.

Selvom det ved hjælp fra ekstern IT-support lykkedes at rense og genetablere tøjbutikkens IT-systemer, løb de samlede omkostninger op i mere end 95.000 kr.

Revisionsfirma utsat for ransomware

Et hackerangreb på et revisionsfirma medførte, at alle computere blev låst. Flere revisorer kunne i flere dage derfor ikke indlevere regnskaber til tiden.

Skadeudgiften for driftstabet løb op i 122.000 kr.

Kilde: TopDanmark²



Det handler ofte om mennesker...

“The Human Firewall”



Sætningen “Det har vi styr på”

.... går desværre igen og igen



Og **basis hygiejnen** er
stadic ikke på plads...

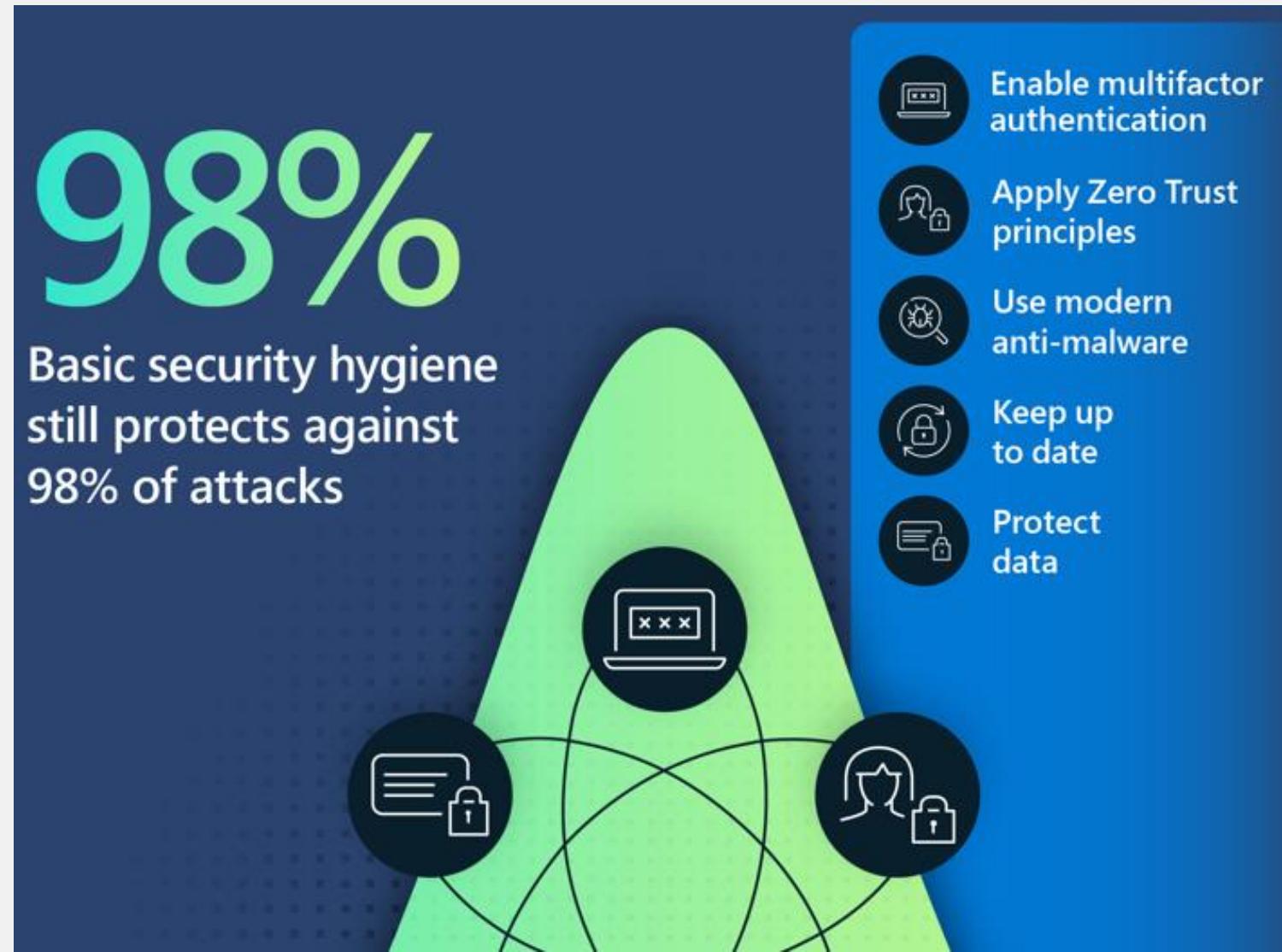


Hvor mange har **MFA** på alle deres konti?

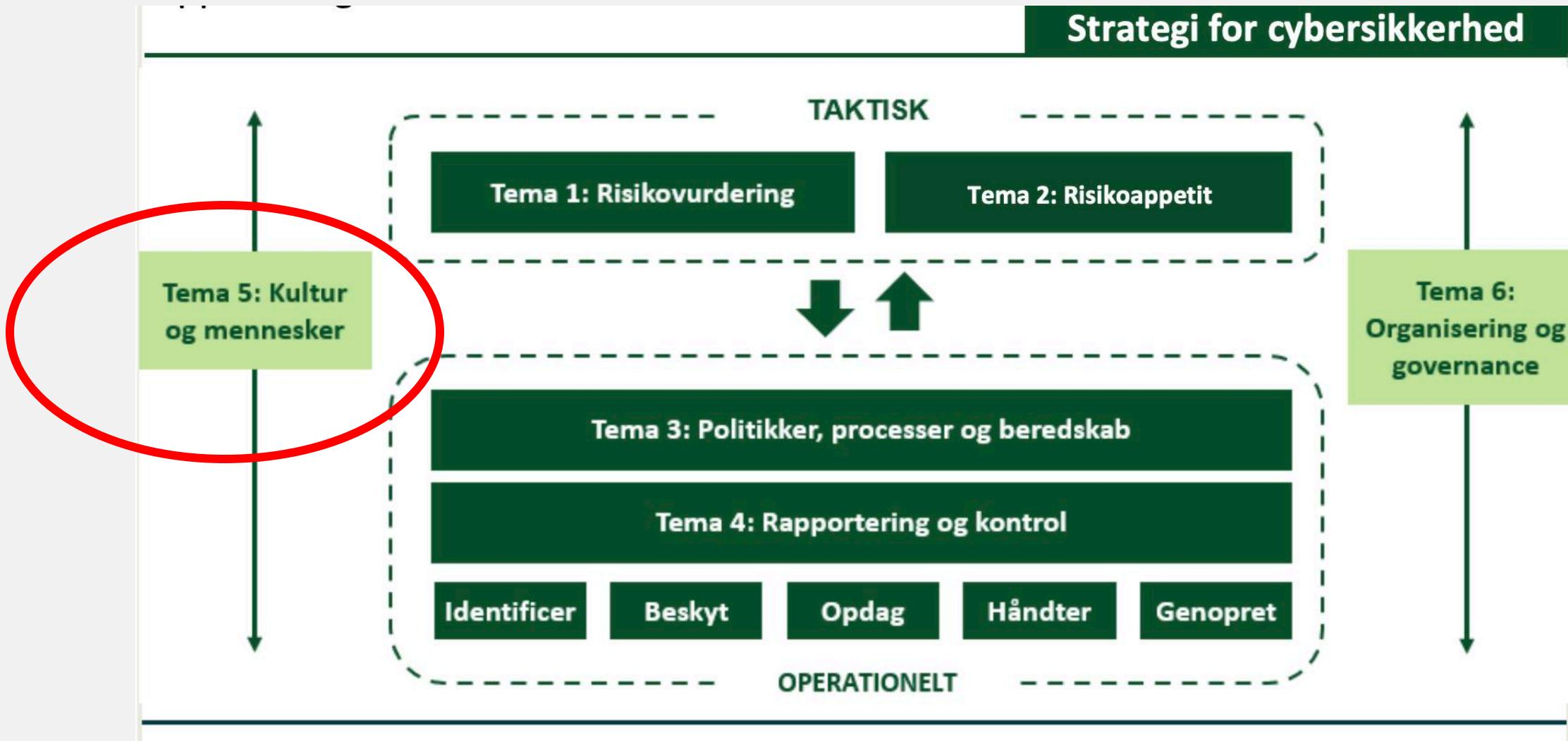


Hvor mange har **forskellige** passwords til
deres konti?

Basis hygiejne gör en forskel



ANBEFALINGER TIL BESTYRELSER



Tema 5: Kultur

– mennesker og træning

Strategier og planer er én ting, men hvis de ikke følges af ledelse og medarbejdere, er man lige vidt.

Medarbejderne er én af de vigtigste kilder til en god sikkerhedskultur og dermed til et højere sikkerhedsniveau.

Inden længe bliver det desuden et lovkrav for ledelser i en lang række virksomheder, at de regelmæssigt skal følge cyberspecifikke kurser.

Der er et behov for træning og awareness programmer for medarbejderne i danske virksomheder og deres ledelser, både i forhold til at dele viden, øge viden og ændre adfærd. Der skal ikke mere end én uopmærksom medarbejder, som trykker på et forkert link, for at der opstår en sikkerhedshændelse.

Den eksplorative vækst i phishing-mails, malware og ransomware, der er rettet mod ledelse og medarbejdere, stiller ikke bare store krav til virksomhedens Sikkerhedsforanstaltninger, men også til den digitale adfærd.

Det kan synes banalt, men for hackere er det meget nemmere at komme ind via (dårlige) IT-vaner, end at skulle hacke sig ind via den "digitale hoveddør".

Insiderproblematikken er reel. Det

estimeres, at 25-35% af alle hændelser kan skyldes medarbejdere – både ubevist (fejl, offer for social engineering mv.) og bevidst (utilfredse medarbejdere, opportunister, svindlere, uhedlige samarbejder mv.).

Der er behov for, at bestyrelsen går forrest i at støtte op om en kultur i virksomheden, hvor sikkerhed kan diskuteres åbent, hvor medarbejderne kan rapportere fejtagelser og brud på sikkerheden, og hvor man lærer af sine fejl. Arbejdet med awareness kan foregå på forskellige niveauer, f.eks. i form af at dele viden internt, øge kendskab/viden og ændre adfærd.

Bestyrelse og direktion behøver ikke kende cybersikkerhed i detaljer, men de bør regelmæssigt følge specifikke kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici og styringspraksisser samt deres indvirkning på virksomhedens drift. Dette bliver også et krav i den kommende NIS2-lovgivning, der vil gælde for en lang række virksomheder.

Som forberedelse til at sparre med og udfordre direktionen indenfor kultur og digital adfærd, kan listen til højre til være til inspiration.

Uddannelse, træning og awareness

- Er der et træningsprogram for, at medlemmer af bestyrelse, direktionen og medarbejdere løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
- Er der et uddannelsesprogram for, at medlemmer af bestyrelse og direktion samt medarbejdere løbende modtager uddannelse i cyberrisici, f.eks. gennem deltagelse i kurser, konferencer og seminarer med fokus på cyberrisiko, cyberkriminalitet og trends og udvikling indenfor virksomhedens branche?

Nøglepersoner

- Baggrundstjejer virksomheden nøglepersoner ved ansættelse?
- Modtager nøglepersoner målrettet træning og uddannelse indenfor cybersikkerhed?
- Er der et specifikt cybersikkerheds awareness program for nøglepersoner eller personer med kritiske funktioner, f.eks. en rejsepolitik i relation til bestemte lande eller en politik for nøglepersoners brug af sociale medier, BYOD (bring your own device)?

Kultur og videndeling

- Foregår der et samarbejde på tværs af organisationen, hvor der deles viden?
- Opfordrer virksomheden sine tekniske specialister til at udveksle viden og erfaringer med medarbejdere fra lignende organisationer for at drage fordel af the 'wisdom of the crowd'

indenfor forebyggelse?

- Benytter den IT ansvarlige sig af netværk og eksterne samarbejder, der kan styrke viden og kompetencer?
- Understøtter ledelsen en positiv sikkerhedskultur, f.eks. ved løbende at informere om cybersikkerhedsstrategien, typen af trusler, og hvordan virksomheden er beskyttet?
- Har virksomheden medarbejdere, den sjældent ser, og ikke har fysisk kontrol over, og som måske har mindre loyalitet?

ANBEFALINGER TIL BESTYRELSER

Strategier og planer er én ting, men hvis de ikke følges af ledelse og medarbejdere, er man lige vidt.
Medarbejderne er én af de vigtigste kilder til en god sikkerhedskultur og dermed til et højere sikkerhedsniveau.
Inden længe bliver det desuden et lovkrav for ledelser i en lang række virksomheder, at de regelmæssigt skal følge cyberspecifikke kurser.

Uddannelse, træning og awareness

- Er der et træningsprogram for, at medlemmer af bestyrelse, direktionen og medarbejdere løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
- Er der et uddannelsesprogram for, at medlemmer af bestyrelse og direktion samt medarbejdere løbende modtager uddannelse i cyberrisici, f.eks. gennem deltagelse i kurser, konferencer og seminarer med fokus på cyberrisiko, cyberkriminalitet og trends og udvikling indenfor virksomhedens branche?

Nøglepersoner

- Baggrundstjekker virksomheden nøglepersoner ved ansættelse?
- Modtager nøglepersoner målrettet træning og uddannelse indenfor cybersikkerhed?
- Er der et specifikt cybersikkerheds awareness program for nøglepersoner eller personer med kritiske funktioner, f.eks. en rejsepolitik i relation til bestemte lande eller en politik for nøglepersoners brug af sociale medier, BYOD (bring your own device)?

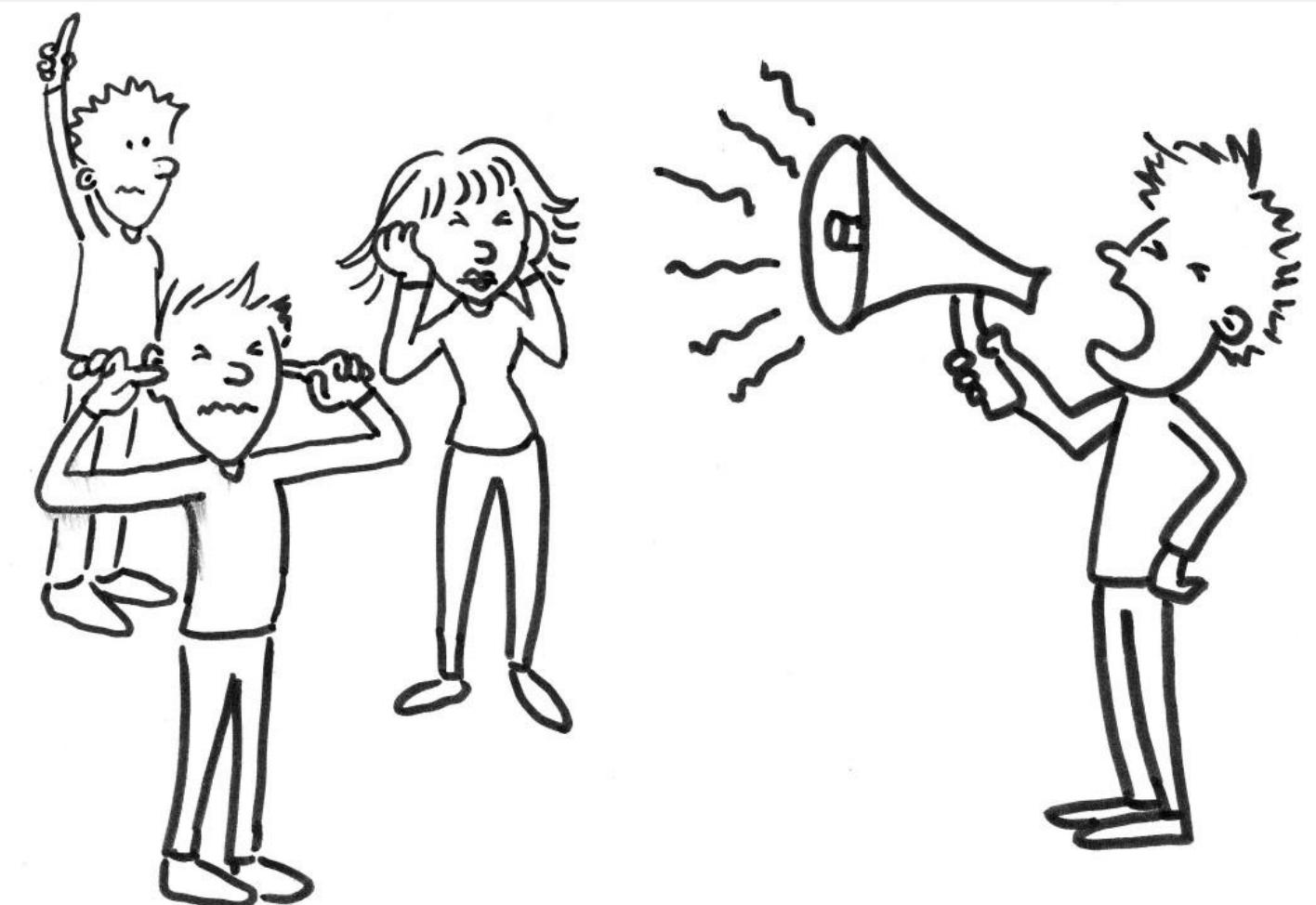
Kultur og videndeling

- Foregår der et samarbejde på tværs af organisationen, hvor der deles viden?
- Opfordrer virksomheden sine tekniske specialister til at udveksle viden og erfaringer med medarbejdere fra lignende organisationer for at drage fordel af the ‘wisdom of the crowd’
indenfor forebyggelse?
- Benytter den IT ansvarlige sig af netværk og eksterne samarbejder, der kan styrke viden og kompetencer?
- Understøtter ledelsen en positiv sikkerhedskultur, f.eks. ved løbende at informere om cybersikkerhedsstrategien, typen af trusler, og hvordan virksomheden er beskyttet?
- Har virksomheden medarbejdere, den sjældent ser, og ikke har fysisk kontrol over, og som måske har mindre loyalitet?



Det handler om at få ledelsen til at forstå hvorfor de skal prioritere ressourcer, og herefter igangsætte de rigtige deltag som man kan måle og evaluere på og som matcher virksomhedens risici...

Masser af relevant teori/viden at sætte i spil





Brug de næste 4 minutter på at tænke over med sidemanden, og liste ned...

Et vellykket phishing angreb, hvilke konsekvenserne kan det føre med sig?

Hvad kan et vellykket phishing angreb betyde?

Et vellykket phishing-angreb kan resultere i:



Identitetstyveri



Tyveri af følsomme data



Tyveri af
kundeoplysninger



Tab af brugernavne og
adgangskode



Tab af intellektuel
ejendom



Tyveri af midler fra
virksomheds- og
kundekonti

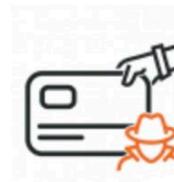
Hvad kan et vellykket phishing angreb betyde?



Reputationsskader



Uautoriserede
transaktioner



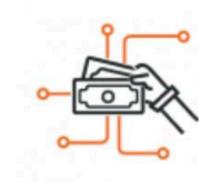
Kreditkortsvindel



Installation af malware og
ransomware



Afgang til systemer til at
iværksætte fremtidige
angreb



Data til kriminelle
tredjeparter



Man skal kunne visualisere og forklare overfor en ledelse, hvad **den forretningsmæssige konsekvens** ved ikke at gøre noget, er...



Hvilke **opgavetyper** vil man typisk skulle varetage?

- At udvikle og implementere awareness-programmer, herunder træningsmaterialer og e-læringsmoduler, der dækker både IT- og OT-sikkerhed
- Organisere workshops, seminarer og kampagner for at øge bevidstheden om cyber- og informationssikkerhed
- Gennemføre phishing-simulationer og andre praktiske øvelser for at teste og forbedre medarbejdernes it-sikkerhedskompetencer
- Udarbejde rollebaseret træning i samarbejde med forretningen, så indsatserne altid er relevante og målrettede
- Monitorere og rapportere awareness-initiativernes effektivitet og løbende tilpasning af strategien
- Rådgive ledelsen og andre interesserter om de bedste metoder til at beskytte virksomhedens aktiver mod cyber-trusler
- Bidrage til at udarbejde politikker og procedurer, der understøtter virksomhedens sikkerhedsmål



Har du lyst til at arbejde med cyber- og informationssikkerhed og derigennem være med til at sikre DMI's samfundsvigtige funktion?

Gå videre for at søge

København
DMI
Kilde : jobfinder

Brænder du for at arbejde med cyber- og informationssikkerhed, der understøtter en moderne virksomhed? Er du samtidig nytænklede, selvstændig og analytisk?

Med solide kompetencer til at formulere dig skriftligt til forskellige fagligheder og organisatoriske niveauer? Så vil et job i enheden Risikostyring og Compliance hos DMI være noget for dig!

Dit nye job

Vi søger en ny kollega til enheden Risikostyring og Compliance, som skal arbejde med cyber- og informationssikkerhed. Du vil få en drivende rolle i at være med til at sikre, at DMI er compliant med de stadig øgede krav til it-sikkerhed i staten.

Implementeringen af de øgede krav skal modsvare trusler fra omverdenen, og sikre at DMI's samfundsvigtige produkter er tilgængelig for Rigsfællesskabet 24 / 7.

Dit arbejde vil være et vigtigt bidrag til implementeringen af kravene på den mest værdiskabende facon og dermed sikre, at omverdenen fortsat har tillid til DMI.

Du vil sammen med dine kollegaer være inde over en bred række af opgaver, som du alt efter erfaring og kompetencer vil skulle drive selvstændigt.

Din stilling vil således blive sammensat af følgende arbejdsopgaver :

- Svare på departementsbestillinger og bestillinger samt statusrapporter fra DMI's tætteste samarbejdsparter i Digitaliseringsstyrelse, Forsvarets Center for Cybersikkerhed (CFCS) mv.
- Indgå i sagsbehandling omkring cyber- og informationssikkerhed ved bla. at understøtte DMI's informationssikkerhedsudvalg med skriftligt materiale
- Gennemføre og facilitere risikoworkshops og konsekvensanalyser for DMI's fagsystemer
- Gennemføre awarenesskampagner om fx informationssikkerhed
- Opdaterer og udarbejde handleplaner og statusrapporter for it-sikkershedskrav
- Udvikle og vedligeholde DMI's informationssikkerhedsledelsessystem

Om dig

Du har en relevant videregående akademisk baggrund og har oparbejdet gode skrivekundskaber. Du behøves ikke at have en IT baggrund, men det er vigtigt at du har en interesse inden for feltet.

Du har en analytisk tilgang til at samle information fra forskellige kilder og finde frem til det essentielle. Du kan tilrettelægge processer samt planlægge og drive dine egne opgaver, så du når deadline.

For at få succes i stillingen skal du trives med at skabe overblik og nedbryde store opgaver, samt selvstændigt indhente nødvendig information og finde frem til løsninger.

Du skal være serviceminded og evne at tale med og forstå specialister fra andre faglige områder end dit eget, ved at forsøge at forstå frem for at blive forstået.

Du skal kunne lide at samarbejde med andre i en travl hverdag samtidigt med, at du formår at være selvstændig og drive dine opgaver fremad, f. eks. mens du venter på input fra kollegaer.

Kompetencer der fx trækkes på?

Kommunikation:

Skriftlig kommunikation

Mundtlig kommunikation

Formidling af komplekse emner til ikke-tekniske brugere

Projektledelse:

Planlægning og koordinering af træningsprogrammer

Implementering af cybersikkerhedsinitiativer

Tidsstyring og ressourceallokering - hvad giver mening, værdi for pengene m.m.

Kreativitet:

Udvikling af engagerende træningsmaterialer som medarbejdere rent faktisk gør brug af

Lave kreative kampagner og oplysningsindsatser der matcher behov

Design af innovative måder at levere information om cybersikkerhed på, så det ikke drukner

Kompetencer der fx trækkes på?

Basal Teknisk Viden:

Forståelse af grundlæggende cybersikkerhedsprincipper så der kan kommunikeres herom

Kendskab til de nyeste trusler og angrebsmetoder

Evne til at oversætte teknisk jargon til ikke-tekniske termer så alle er med

Analytiske Evner:

Evaluering af hvilke sikkerhedsrisici og sårbarheder der bør fokus på

Analyse af brugeraadfærd og reaktion på træning (dataanalyse)

Udarbejdelse af rapporter til ledelse

Social Engineering:

Forståelse af brugeraadfærd så man kan kommunikere effektivt

Identifikation af potentielle svagheder i organisatorisk adfærd

Gennemførelse af phishing-simulationer

Kompetencer der skal trækkes på?

Ledelsesengagement:

Engagement af ledelse og interesserter i cybersikkerhedsinitiativer

Opbygning af støtte og forståelse på tværs af organisationen

Skabe en kultur med cybersikkerhedsbevidsthed fra toppen

Didaktik

Eksperimentering med nye undervisningsmetoder

Implementering af nye digitale løsninger ifb med træningsprogrammer

Tilpasning til nye trusselsscenarioer og trends

Samarbejdsevner:

Samarbejde med tværfaglige teams

Partnerskab med eksterne sikkerhedsekspertir og organisationer

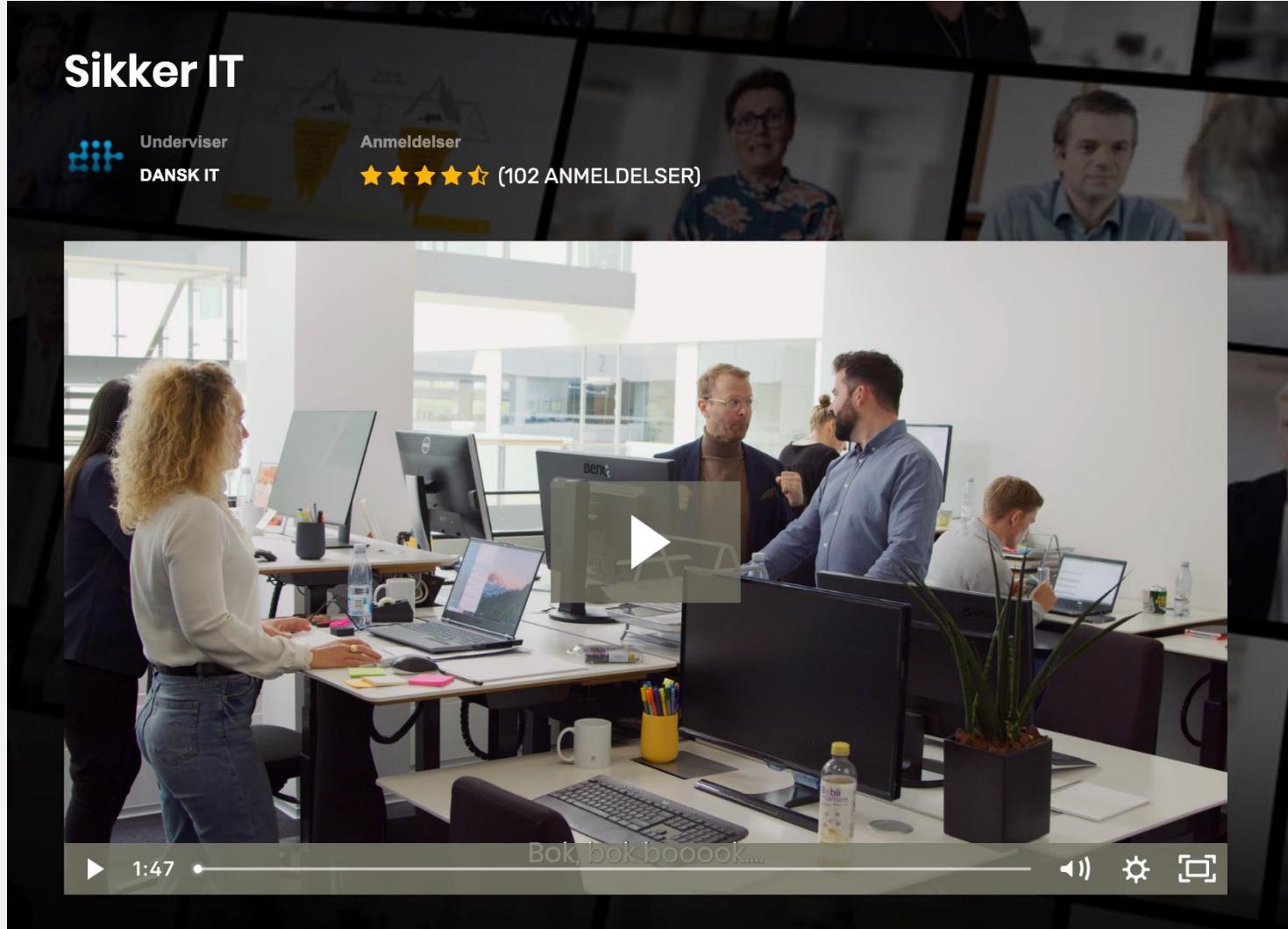
Skabe et netværk inden for cybersikkerhedsfællesskabet

A vertical decorative bar on the left side of the slide features a complex, abstract design in shades of blue. It includes a grid of light blue lines, several curved white lines forming a path or trajectory, and numerous small glowing blue and white dots, suggesting a network or data points.

One size does not fit all...

E-læring

<https://www.golearn.dk/it-sikkerhed-online-kursus/>





Vi skal uddanne vores medarbejdere.

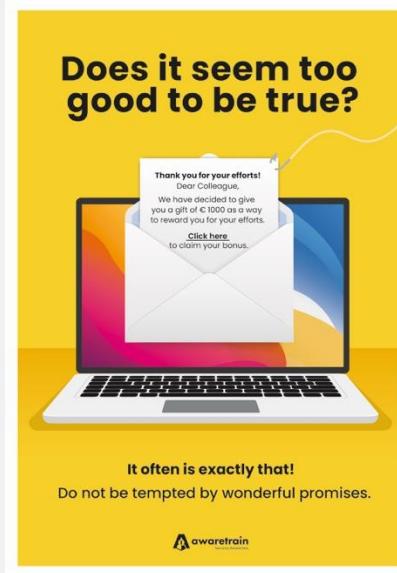
De er “the weakest link” og vores “human firewall”...

Men hvordan?

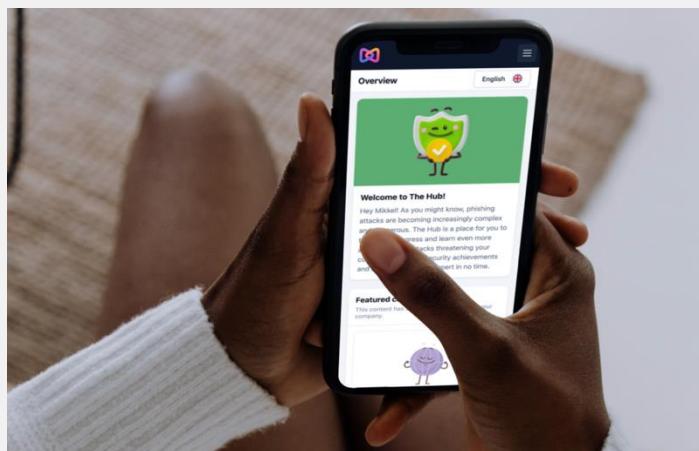
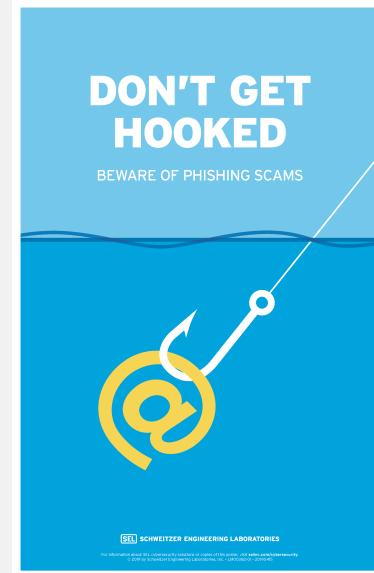
Awareness kommer i mange former



Fysiske kortspil



Plakater

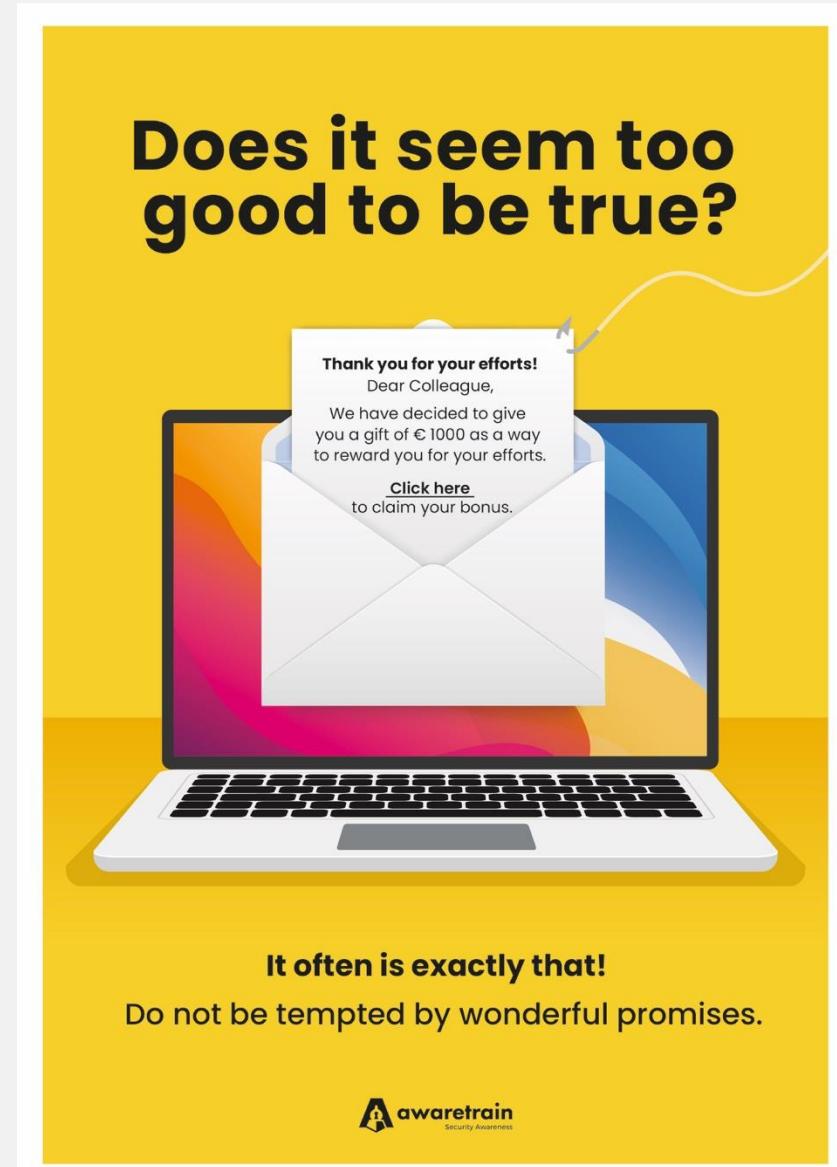
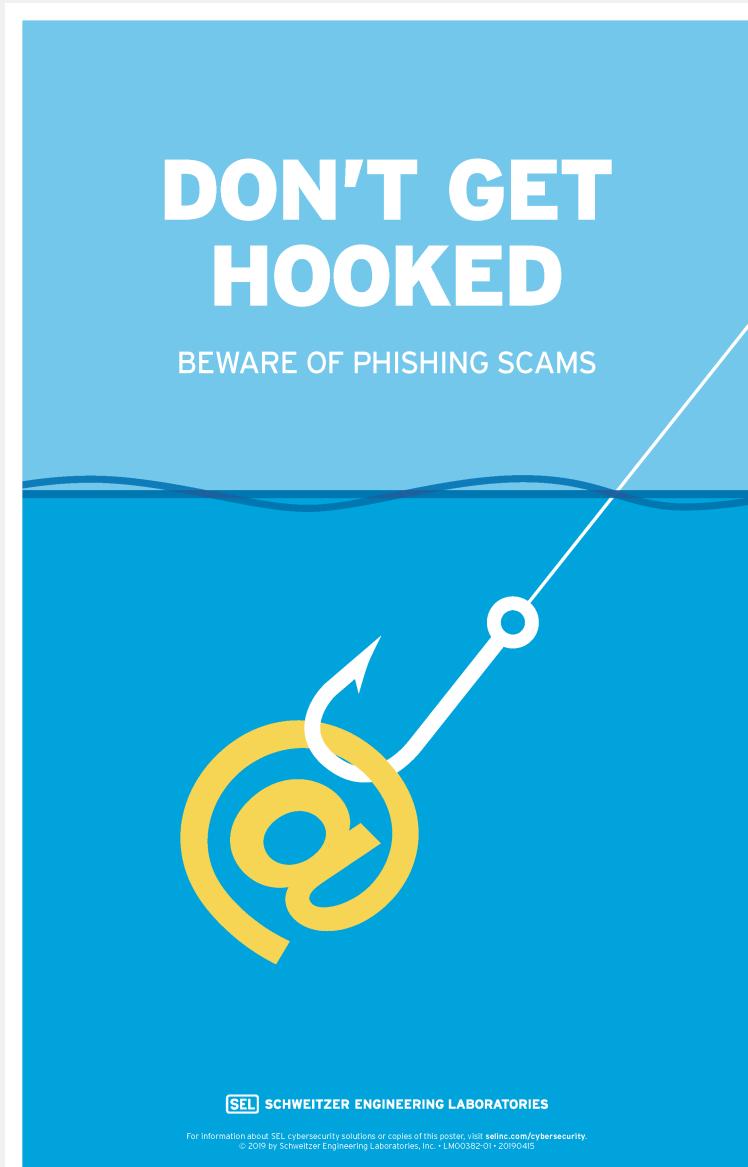


Interaktiv læring

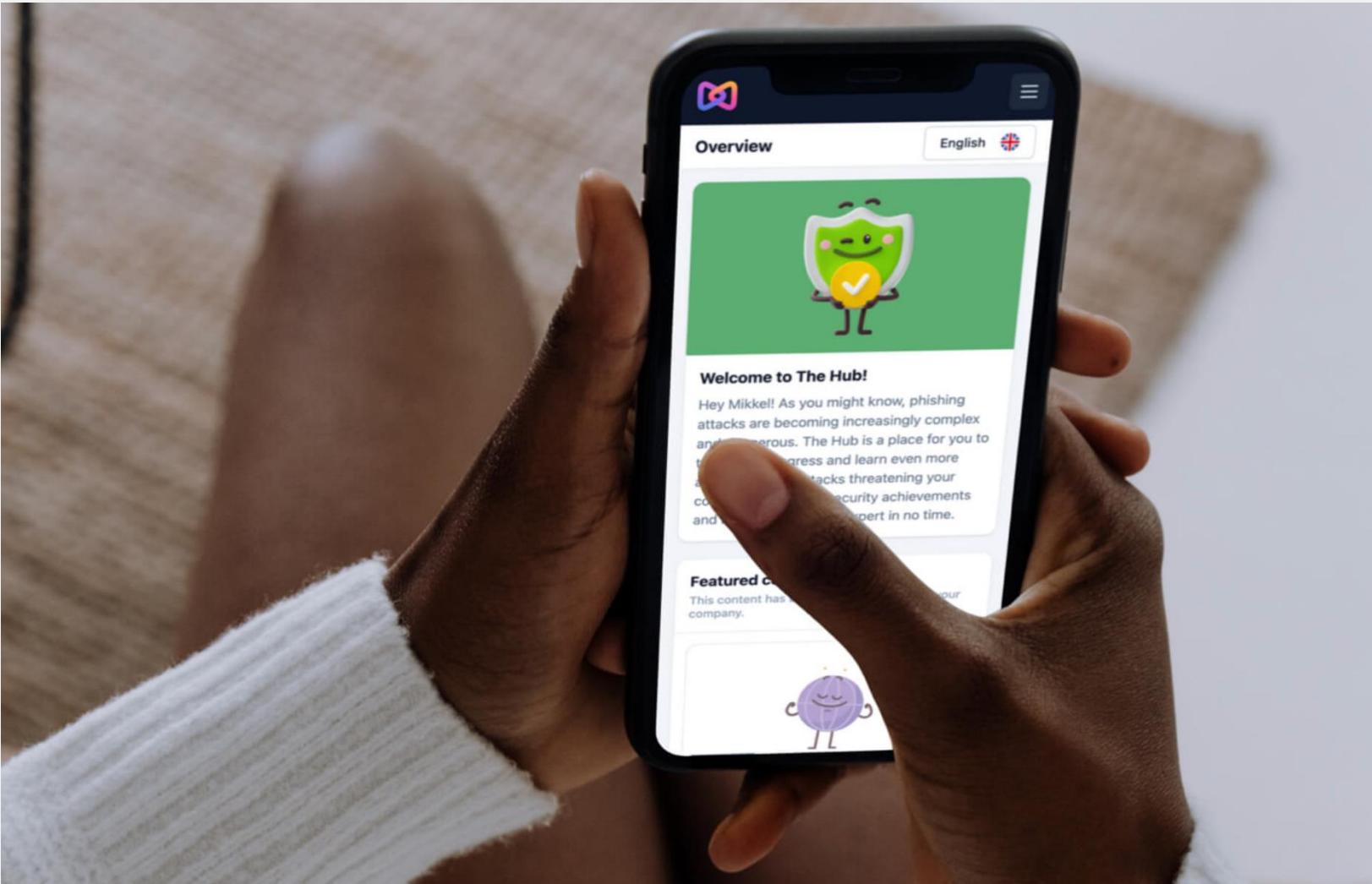
Kort-spil



Kreativ kommunikation

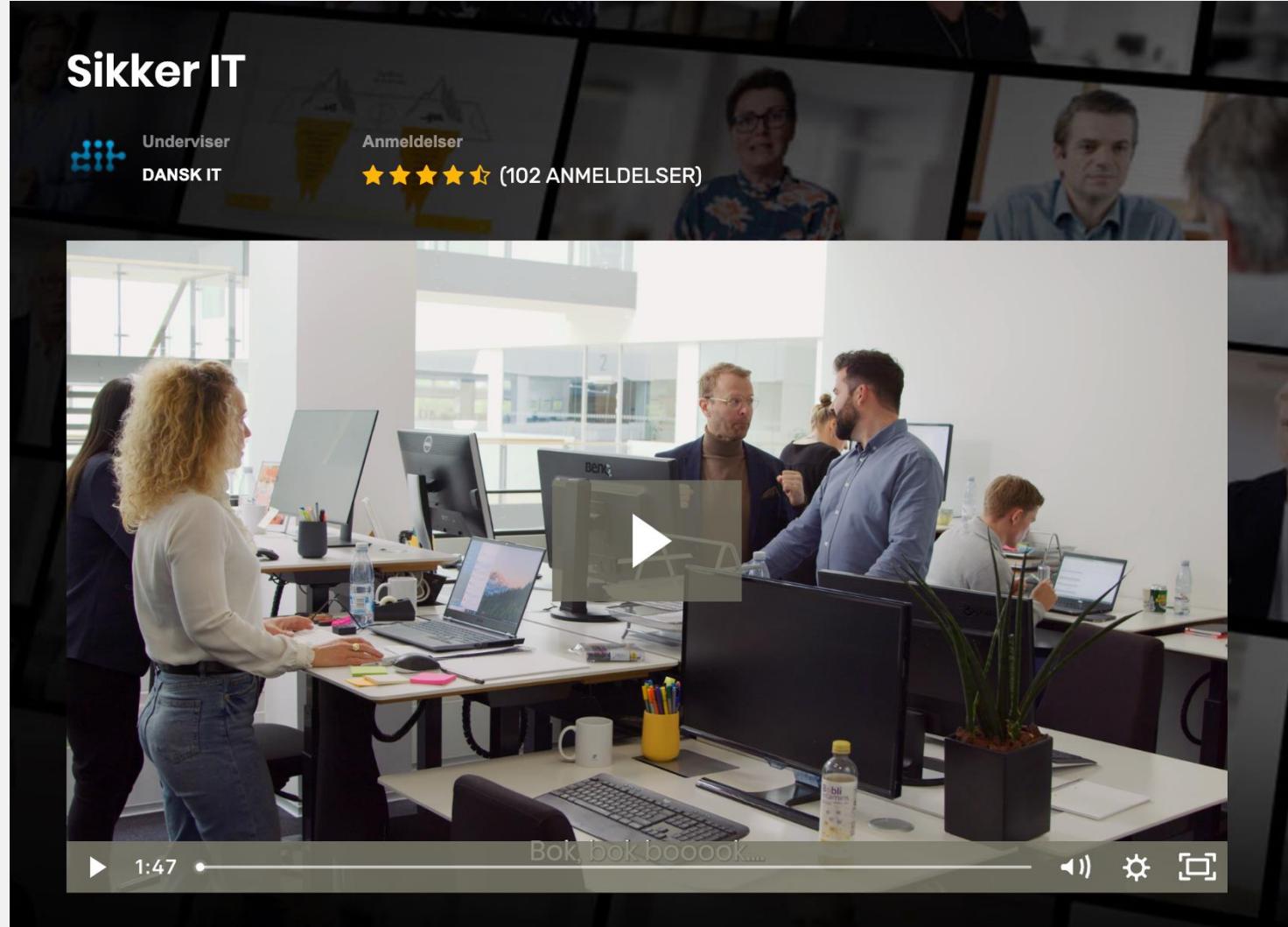


Mikrotræning



E-læring

<https://www.golearn.dk/it-sikkerhed-online-kursus/>





**Har I selv modtaget træning på det
sted I arbejdede/studerede, og
hvordan virkede det på jer?**

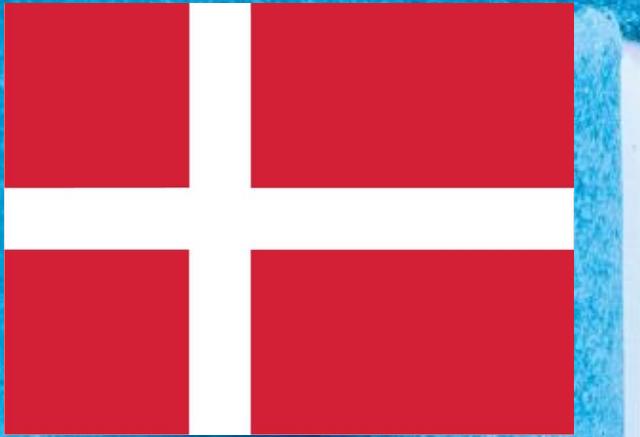


Cyber Awareness

En vigtig (men svær) prioritering

BRUG 2 MINUTTER MED JERES SIDEMAND OG DISKUTER SPØRGSMÅLET!

Vores danske mentalitet er vores største "udfordring"



TILLID

Vores danske mentalitet er vores største "udfordring"

Hvad er tailgating, og hvorfor truer det cybersikkerheden på arbejdspladsen?

JAMES MACKAY METABLOG OM CYBERSIKKERHEDS-AWARENESS



Hackerne går efter **"weakest link"**



Hackere arbejder **organiseret**



Når vi træffer **beslutninger...**

Hurtig
Impulsiv
Emotionel
Ubevidst
Hverdag
90 %



Langsom
Analytisk
Rationel
Bevidst
Komplekst
10 %



På trods af sætningen “Det har vi styr på”

.... går igen og igen

Ser vi stadig rigtig mange eksempler...

Eksempler fra hverdagen...

Anna Thygesen • 2.
Trusted advisor, kommunikationsrådgiver og CEO, We...
2u •

Skader svindelsagen mit brand?
I fredags valgte jeg at dele en relativt grænseoverskridende oplevelse om at jeg for 2 uger siden blev svindlet og mistede alle mine penge. ... mere

Svindlet: Alle pengene er væk

89 kommentarer • 4 anannonser

755

Anna Thygesen • 2.
Trusted advisor, kommunikationsrådgiver og CEO, We...
1u •

Update: [Danske Bank](#) har overført alle mine penge minus en selvisiko på 8.000 kr. til min konto. Tak for god support og service 😊
Også tak til politiet, NSK og borgerservice for hjælp og forståelse.
Tak til alle for de støttende, rørende og søde beskeder og hilsner. Det betyder meget.

Men allerlest tak til alle jer, der har bidraget med vilde beretninger om personlige oplevelser med svindel og hacking. Det er vigtigt at vide at man ikke er helt alene.

Og endelig tak for at lade mig udbrede budskabet om at svindel og hacking rammer ALLE aldre og ALLE sociale klasser og om at vi skal kunne tale om det her på en faldomsfri måde.

Husk at være skeptisk, når det handler om at politi eller bank vil noget med dine penge og husk aldrig at udlevere koder eller passwords 🔥

Kærligst Anna 😊

DIGITAL SVINDEL KONTOEN BLEV TOMT PÅ ET OJEBLIK

De sidste par uger har været decideret rystende for den kendte kommunikatør Anna Thygesen.

Derfor ønsker hun nu at komme med et opråb, så andre i hendes situation kan slippe bedre, end hun selv er endt med.

B.T. har tidligere beskrevet, hvordan Anna Thygesen, der blandt andet er kendt fra podcasten 'Det, vi taler om', har været utsat for et større svindelnummer.

Nu fortæller hun, hvordan de seneste uger har været hårde for hende psykisk.

Det var et opkald med en bankmand, der endte med at få voldsomme konsekvenser for kommunikatøren.

Eller i hvert fald, hvad hun troede, var en bankmand.

For efter at have stoppet hvad der blev præsenteret som en mistænkelig overførsel, kunne hendes mand pludselig fortælle, at fælleskontoen var fuldstændig ribbet.

Til B.T. fortæller Anna Thygesen, hvordan hun på intet tidspunkt før det øjeblik mistænkte, at der skulle være noget galt.

»Nummeret ligner min banks, og de har et sagsnummer til politiet. Der er ikke noget, der på noget tidspunkt får mig til at tænke, at der er noget galt,« siger hun.

Svindlerne bruger ifølge kommunikatøren flere greb, der gør, at hun ikke når at tænke, at der er noget galt.

Eksempler fra hverdagen...

Fupkøbere sender phishinglinks til falske fragt- eller betalingssider

Flere sælgere på DBA bliver kontaktet af fup-købere - Dette kan både være via sms, e-mail, WhatsApp eller i 'Spørgsmål & Svar'-dialogen på annoncen.

De falske købere sender et phishinglink som enten ligner DBA eller fragtudbydere (UPS, DAO, GLS eller PostNord). Ens for dem alle er, at du bliver bedt om at oplyse kortoplysninger for at modtage betaling.

Disse sider er forsøg på phishing.

DBA tilbyder **ikke** 'DBA betaling' eller arrangerer fragt af varer.

Har du indtastet dine kortoplysninger, skal du straks spærre dit betalingskort hos dit pengeinstitut. Har du oplyst dit MitID skal dette også spærres.

Eksempel på henvendelser fra svindlerne:

"Jeg har allerede betalt for leveringen, og du skal få pengene fra linket. Kureren ringer til dig i morgen."

"Kan du sende mig din e-mailadresse? Jeg betaler for leveringen på hjemmesiden og angiver alle mine kontaktoplysninger der."

Kendetegn - Dette skal du være opmærksom på:

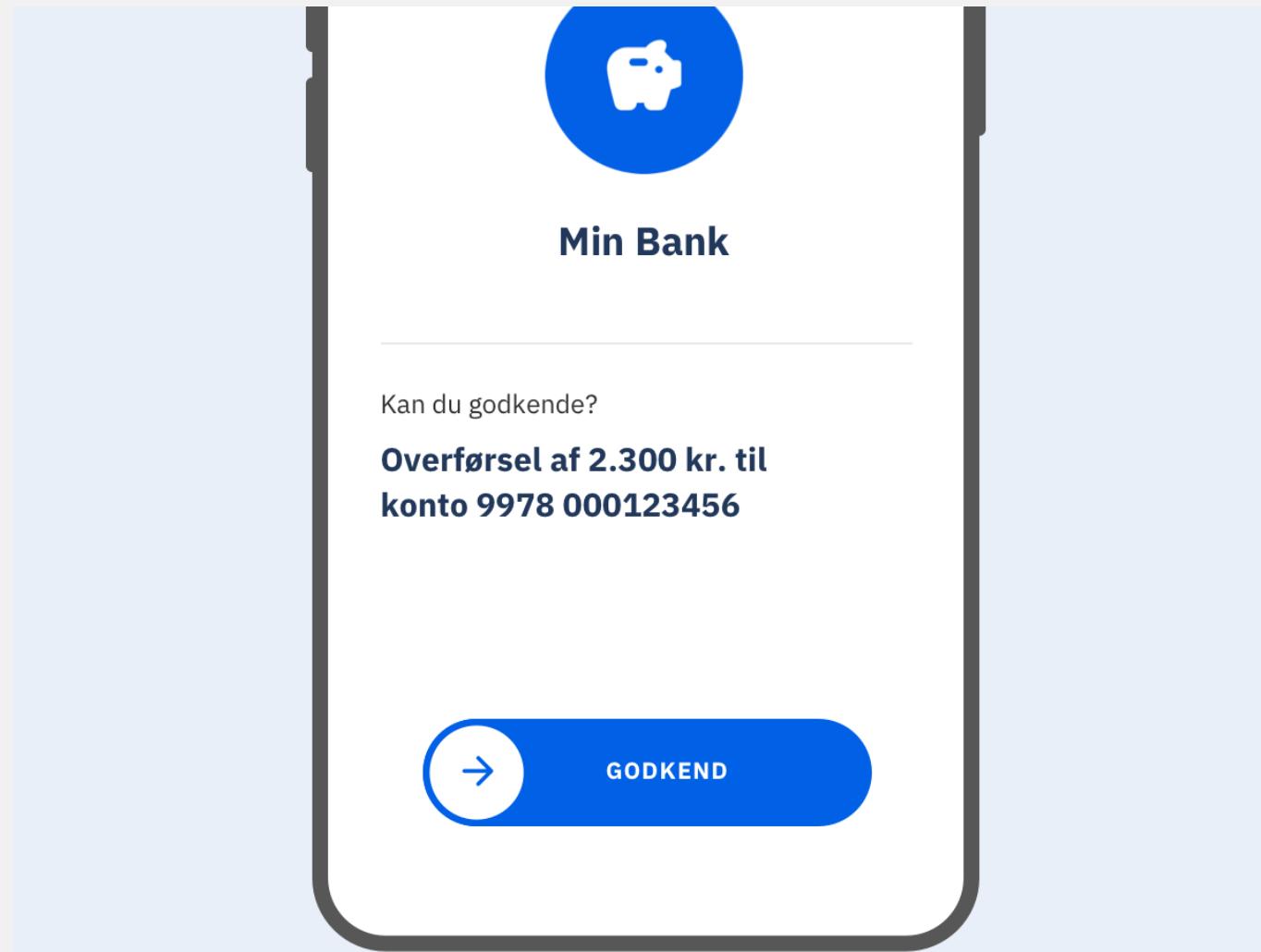
- Dialogen foregår typisk på dansk
- Ofte forsøger svindleren af få oplyst din mailadresse, så I kan kommunikere udenom DBA - Dermed kan dialogen fortsætte selvom DBA har blokeret svindleren på sitet
- 'Køber' ønsker at få varen leveret med fragtfirma - ex. GLS eller PostNord)
- Der sendes et link, hvor du skal oplyse dine kreditkortoplysninger eller login til DBA

3 gode råd:

1. Tjek køberens profil - Er profilen nyoprettet og ikke MitID-valideret skal du være obs
2. Hold dialogen på DBA - Flyt ikke samtalen til f.eks. e-mail, WhatsApp eller Messenger
3. Oplys aldrig logindata eller kortoplysninger via link

Modtager du betaling via MobilePay eller kontooverførsel, så tjekker at pengene er indsat på din konto inden du sender varen.

Eksempler fra hverdagen...



Eksempler fra hverdagen...

Opmærksomhed



Politi Direktor <politidirektor1@gmail.com>

Til



– Politiets hasteordre.jpg
844 KB

Politiets Hasteordre,

Opmærksomhed: Til Hvem Det Måtte Vedrøre,

Du har fået mandat med øjeblikkelig virkning af Rigs-politiet til at besvare vedlagte stævning inden for 48 .

Hvis de ikke er i stand til at svare, har vi intet andet valg end at træffe retslige foranstaltninger mod dem.
timer

Med venlig hilsen,

Lasse Boje Nielsen
Politidirektør
Enhed For Særlig Kriminalitet
Ejby Industrivej 125-135
2600 Glostrup
E-mail: politidirektor1@gmail.com
EAN-nummer: 5798000082366

Eksempler fra hverdagen...

Politiet advarer mod Airbnb-svindel

7. apr 2017 kl. 22.28



Mest sete p



Eksempler fra hverdagen...

INDLAND

Telefonsvindel mod ældre er et stigende problem: Sonja lagde 19.000 kroner under dørmåtten

Antallet af anmeldelser er steget med 55 procent på ét år.



83-årige Sonja Jensen blev af en telefonsvindler overtalt til at udlevere 19.000 i kontanter. (© DR Nyheder)

Eksempler fra hverdagen...

SENESTE NYT | I GÅR KL. 15:21

Flere ældre snydt på Fyn: Politiet efterlyser nu svindler

LÆS OP ORDBOG TEKST

AF
Thomas Bansø

Flere sager om snyd mod ældre borgere får nu Fyns Politi til at komme med en efterlysning.

Personen udgiver sig for at være fra sikkerhedsafdelingen fra en bank, hvor han fortæller borgeren, at der lavet transaktioner til udlandet.

Herefter sender manden en person, der skal deponere den ældre borgers dankort. I de tilfælde er der hævet penge på kortet, og der er også blevet udleveret kontanter fra den ældre person til manden.

- Der er tale om en meget udspekuleret form for bedrageri, der går hårdt ud over vores ældre borgere. Det er lykkedes en eller flere gerningspersoner at tilegne sig til flere tusinde kroner, siger vicepolitiinspektør ved Fyns Politi Michael Lichtenstein

Den efterlyste beskrives som mand, 16-22 år gammel, der bærer en sort eller mørkeblå Peak Performance jakke, blå jeans og sorte sko,

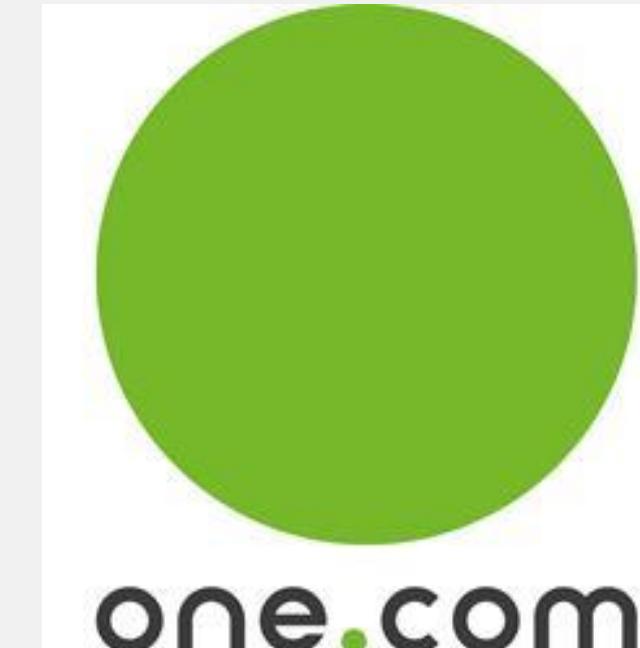
Har man oplysninger i sagen, kan politiet kontaktes på 114.

FACEBOOK TWITTER KOPIER LINK

Eksempler fra hverdagen...

Vigtigt: one.com vil **aldrig** bede om din adgangskode. Hvis du modtager en e-mail, hvor du bliver bedt om at angive din kontaktmail og adgangskode, anbefaler vi at slette den med det samme eller flytte den til spam-mappen. Skulle one.com få brug for din adgangskode til fejlfindingsformål, vil dette kun ske efter forudgående aftale med dig.

Hvis du allerede har svaret på e-mailen og udleveret personlige oplysninger og/eller kortoplysninger, vil vi ráde dig til at kontakte din bank hurtigst muligt og få spærret dit kort.



Ditte Vinterberg Weng · 2.

Journalist for cybersikkerhed hos Computerworl...
1u ·

+ Følg ...

Jeg fnisede, da hun sagde, jeg var blevet offer for svindel...

Ved siden af mit arbejde som journalist, har jeg en virksomhed, hvor jeg laver livshistorier om til lydfortællinger. Til den virksomhed hører et domæne, som jeg har hos One.com. Og særligt i den mail, der er knyttet til det domæne (ourstory.dk), modtager jeg en del svindel-mails om ubetalte fakturaer, som ligner at de er fra One.com.

Nu gik jeg så i en af dem, og kom til at indtaste mine kontooplysninger i et system, der - og props for det store arbejde med at få det til at se så ægte ud - komplet ligner one.coms eget system.

Men da jeg havde tastet oplysningerne ind, og den så bare stod og tænkte i flere minutter blev jeg mistænkelig, og ringede til One.com. Og i det jeg stillede spørgsmålet, fik jeg øje på sidste linje i den mail, jeg var kommet til at reagere på - uden at læse det hele:

"Tak fordi du er medlem af én familie".

Jeg fnisede mens den søde medarbejder i telefonen fortalte, det jeg nu allerede vidste, at det desværre var svindel.

Så jeg skyndte mig at ringe til min bank, mens jeg på min app spærrede mit kort. Stadig fnisende.

Jeg orkede ikke lige at ringe for at dobbeltjekke den faktura, jeg havde fået sendt til min mail... så nu sidder jeg med et spærret kort og 8 til 10 dag, til jeg modtager det nye. Og så skal jeg lige holde øje med min konto for en sikkerheds skyld de næste dage.

Det er ren held, at jeg har kontanter til at dække de næste 10 dage. Ellers er det ikke sikkert, at min reaktion, da jeg fandt ud af at det var svindel, havde været den samme.

Men altså... hvorfor fanden ringede jeg ikke bare til one.com til at starte med, da jeg var i tvivl. Hermed har jeg forhåbentlig nu lært at følge de sikkerhedsråd, jeg har skrevet kilometer lange linjer om i mine egne spalter. 😊

God dag og tak fordi du er en del af én familie ❤️

Maja Øvlisen og 102 til

21 kommentarer · 1 genopslag



Eksempler af erhvervsmæssig karakter...

CEO-Fraud

ONDSINDET PHISHING HAR RAMT BRUGERNE AF MICROSOFT 365

I den sidste tid er en række danske advokatfirmaer blevet snydt af fupmails, som desværre har vist sig at være mere ondsindede end først antaget.

[Se nyhed fra 20. januar med eksempel på fupmails](#)

Fupmails, der snyder modtagerne, har de seneste uger målrettet deres beskydninger mod danske virksomheder og helt specifikt også mod advokatbranchen. Fænomenet kendes også som fraud-kampagner og kaldes teknisk et "Business Email Compromise" (BEC).

I første omgang fik vi kendskab til, at en række advokatvirksomheder havde fået aktiveret fupmails. Disse spredte sig yderligere ved, at der blev sendt fupmails til de mailadresser, der var på de enkelte brugeres mailkonti. Der var tvivl om, hvad det derudover kunne betyde. Vi har nu fået nærmere indsigt i dette fra et par af de ramte advokatfirmaer. Også sikkerhedsfirmaet CSIS har givet os indsigt i omfanget af angrebet og hvilke konsekvenser, det kan medføre. Der er dermed tale om ondsindet phishing og ikke blot malware!

Et BEC-angreb udføres typisk i flere etaper:

1. Kompromittering af e-mailkonto via phishing mod Microsoft Office 365-konti
2. Overvågning af e-mails, opsætning af e-mailregler mv
3. Eksekvering af selve BEC-angrebet ved brug af informationer fra den kompromitterede e-mailkonto

CSIS oplyser, at de har fået indsigt i et angreb, som endnu ikke er færdigudført, da de IT-kriminelle typisk bruger uger eller måneder på at planlægge hele angrebet. CSIS ved, at der allerede har fundet flere succesfulde angreb sted, men at det med stor sandsynlighed kun er starten.



**CFCS vurderer også at phishing er et
centralt område der bør fokuseres på...**

Cybertruslen fra phishing-mails

Cyberangreb, som indledes med en phishing-mail, er meget udbredte og fører til tab af penge, data og omdømme eller alvorlige kompromitteringer af it-netværket hos myndigheder og virksomheder. Det er derfor vigtigt at være opmærksom på truslen og indføre passende forholdsregler for at imødegå den.

Hovedvurdering

- CFCS vurderer, at phishing ved hjælp af e-mails udgør en vedvarende og alvorlig cybertrussel mod alle myndigheder, virksomheder og borgere i Danmark.
- Det er sandsynligt, at de fleste cyberangreb i dag indledes med en phishing-mail.
- CFCS vurderer, at op mod 80 procent af de e-mails en organisation modtager udefra kan være uønskede eller direkte skadelige, og at større organisationer dagligt modtager phishing-mails.
- Phishing anvendes af både cyberkriminelle og statslige hackere. CFCS vurderer, at de fleste phishing-mails udgår fra organiserede kriminelle, som også leverer infrastruktur, værktøjer og tjenester, som understøtter phishing.
- Et phishing-angreb kan potentielt skade samfundet, hvis angrebet rammer en myndighed eller virksomhed, som leverer samfundsvigtige ydelser, tjenester eller lignende.
- CFCS vurderer, at de fleste phishing-mails fungerer i samspil med en skadelig hjemmeside, der efterligner en legitim hjemmeside. Ved at lukke eller blokere adgangen til hjemmesiden kan den skadelige effekt af den specifikke phishing-mail fjernes.

Indhold

Indledning	3
Overordnede anbefalinger.....	5
Phishing	6
Hvad bruges phishing til?.....	6
Opdag tegn på phishing.....	7
Gør det svært at lykkes med phishing-mails.....	8
Når der modtages mails.....	8
Installer antivirus og brug mailfiltre.....	8
Behandl indkommende mails i henhold til afsenderdomænets DMARC-politik.....	8
Ved tvivl få afsenders identitet bekræftet.....	9
Gør det nemt at rapportere om mulige phishing mails	9
Minimer mængden af tilgængelig information om organisationen	10
Hav processer og kend dem	10
Når der udsendes mails	11
Anvend DMARC, SPF og DKIM, og bekæmp spoofing	11
Undgå at bruge phishing-lignende kommunikation	11
Begræns konsekvenserne af ikke opdagede phishing-angreb	13
Installer sikkerhedsopdateringer og anvend application control.....	13
Hold antallet af brugere med lokale administratorrettigheder på et minimum	13
Implementer tiltag, der beskytter brugere mod kendte ondsindede hjemmesider... ..	13
Brug flerfaktor-autentifikation	14
Håndter phishing-angreb	15
Logning	15
Hændelses- og beredskabsplaner.....	15
Referencer.....	16



CENTER FOR
CYBERSIKKERHED

Vil du hjælpe CFCS med det nationale overblik på phishingområdet, så kan du nu indberette phishingmails til CFCS

Har du eller din virksomhed modtaget en e-mail, som kunne være et forsøg på phishing, så kan du indberette e-mailen til Center for Cybersikkerhed.

Phishing udgør en vedvarende og alvorlig trussel mod alle myndigheder, virksomheder og borgere i Danmark. Mængden af phishingmails er så stor, at mange organisationer oplever daglige forsøg på kompromittering.

Spear Phishing...



PHISHING

IS A BROAD, AUTOMATED ATTACK
THAT IS LESS SOPHISTICATED.

SPEAR-PHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC
EMPLOYEE & COMPANY



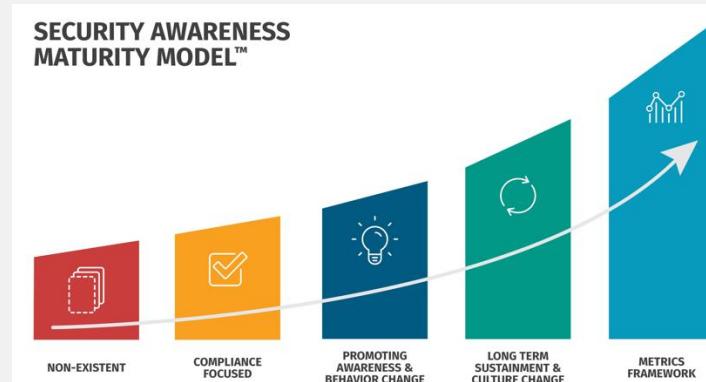
**Har I selv været ude for et forsøg og
hvordan var det sat op?**

Blev der gjort brug af spear-phishing?

BRUG 5 MINUTTER MED JERES SIDEMAND OG DISKUTER SPØRGSMÅLET!

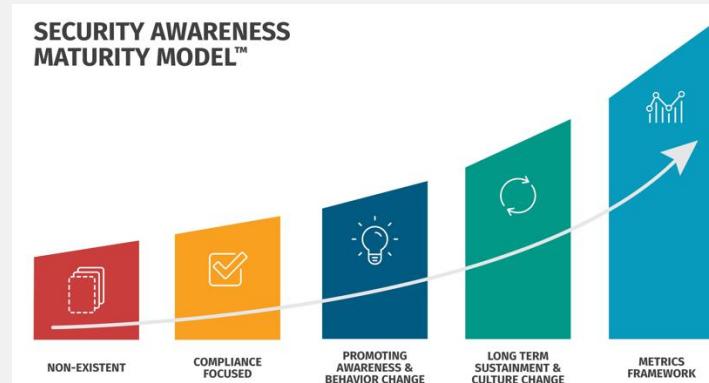
2 modeller

- Security Awareness Maturity Model (SAMM)
- Confidentiality-Integretity-Availability (CIA)



2 modeller

- Security Awareness Maturity Model (SAMM)
- Confidentiality-Integretity-Availability (CIA)



Security Awareness Maturity Model (SANS)

SECURITY AWARENESS MATURITY MODEL™

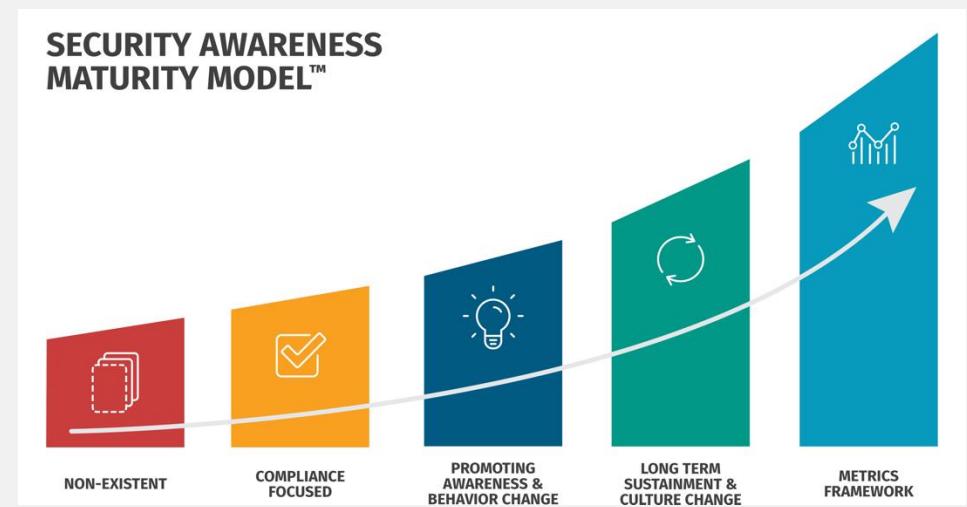


Security Awareness Maturity Model (SANS)

En modenhedsmodel, der evaluerer organisationers niveau af modenhed inden for cybersikkerhedsbevidsthed, og hjælper med at identificere områder, hvor forbedringer er nødvendige.

Den giver altså struktureret tilgang til at evaluere cybersikkerhedsbevidsthed og identificere specifikke områder, hvor organisationen kan forbedre sig.

Ved at definere klare modenhedsniveauer er det også en model der kan bruges til at tale om modenhed med ledelsen, og hvor man ønsker at bevæge sig hen.



CIA-modellen





Vi bliver nød til at være **konkrete** i vores kommunikation, og hjælpe med at tage bedre valg, hvis vi skal ændre adfærd



15 emner man kan sætte fokus på indenfor cyber awareness...

Det afhænger af virksomheden, trusselsbilledet, sårbarheder - og dermed risici ift hvad der giver mening at sætte fokus på..

VPN

Hvad det er: En VPN (Virtual Private Network) er en sikker forbindelse, der krypterer dine internetaktiviteter, mens sikkert wifi refererer til beskyttede trådløse netværk.

Eksempel: Når du bruger offentlige wifi-netværk på caféer, sikrer en VPN, at dine data forbliver private, hvilket beskytter mod potentielle hackere.

Vi vil hjælpe til at adfærdens er følgende...: Når du sidder på din yndlingscafé og arbejder på din bærbare computer, aktiverer du altid din VPN-forbindelse, selvom cafeens wifi-netværk er tilgængeligt. På den måde kan du trygt håndtere følsomme oplysninger uden at bekymre dig om potentielle hackere, der sniffer efter data.

Hvorfor er det så svært at få folk til at anvende VPN?

Des- og misinformation

Hvad det er: Desinformation er bevidst spredning af falske oplysninger, mens misinformation er fejlagtige oplysninger uden ond hensigt.

Eksempel: Deling af falske nyheder på sociale medier kan skabe forvirring og underminere tilliden til pålidelige kilder.

Vi vil hjælpe til at adfærdens er følgende...: Du modtager en besked på sociale medier om et påstået sundhedstip, der hævder at drikke en usædvanlig blanding af ingredienser vil kurere alle sygdomme. Du husker at tjekke kilden og opdager, at den er upålidelig, så du undlader at dele det for at forhindre spredning af falsk information.

Hvorfor hopper folk på "falsk information"?

Minimer digitale fodafttryk

Hvad det er: At reducere det digitale fodafttryk indebærer at begrænse mængden af personlige oplysninger online.

Eksempel: At være opmærksom på, hvilke personlige oplysninger du deler online, kan mindske risikoen for målrettede angreb på dine data.

Vi vil hjælpe til at adfærdens er følgende...: Når du opretter profiler på sociale medier, deler du kun de nødvendige oplysninger og undgår at give adgang til personlige detaljer som din hjemmeadresse eller telefonnummer for at beskytte din privatliv.

Hvorfor deler folk i vildskab på sociale medier?

Malicious Attachments

Hvad det er: Onde vedhæftede filer er filer, der indeholder skadelig software, ofte sendt via e-mails eller beskeder.

Eksempel: Modtagelse af en e-mail med en mistænkelig vedhæftet fil bør undlades for at undgå potentielle sikkerhedsrisici.

Vi vil hjælpe til at adfærden er følgende...: Du modtager en e-mail med en vedhæftet fil fra en ukendt afsender. I stedet for at åbne filen, rapporterer du straks e-mailen som spam og undgår at udsætte din enhed for mulig malware-infektion.

Hvorfor downloader medarbejdere stadig filer der ser mistænkelige ud?

Lås skærmen

Beskrivelse: At låse skærmen, når en medarbejder forlader sin arbejdsstation, er afgørende for at forhindre uautoriseret adgang til følsomme oplysninger.

Eksempel: Brug altid windows-tast + L

Vi vil hjælpe til at adfærdens er følgende...: Medarbejderen forlader aldrig computeren, med åben skærm, men bruger altid windows-tast + L til at låse sin computer med.

Hvorfor klikker folk ikke Windows-tast + L når de forlader PC'en?

Ukorrekte eller usikre links



Hvad det er: Links til upålidelige eller falske websteder kan føre til sikkerhedstrusler som phishing eller malware.

Eksempel: Et link i en e-mail, der ser legitmt ud, men faktisk fører til et falsk websted, kan narre folk til at dele fortrolige oplysninger.

Vi vil hjælpe til at adfærden er følgende...: Du modtager en e-mail, der hævder at være fra din bank og beder om at klikke på et link for at opdatere dine bankoplysninger, du finder det mistænksomt og rapporterer mailen som phishing.

Hvorfor klikker folk på links der ser mærkelige ud?

MFA

Hvad det er: Multifaktorautentifikation kræver yderligere trin ud over brugernavn og adgangskode for at bekræfte identiteten.

Eksempel: Udeover indtastning af adgangskoden kan MFA kræve en bekræftelseskode sendt til en mobiltelefon, hvilket øger sikkerheden betydeligt.

Vi vil hjælpe til atadfærdens er følgende...: At du på alle dine konti har oprettet MFA, du mener det skal prioriteres både på private og arbejdskonti.

Hvorfor har folk stadig ikke MFA på alle konti?

Samtaler i det offentlige rum

Hvad det er: Diskussioner i offentlige rum indebærer at være opmærksom på, hvilke oplysninger man deler og med hvem, især når samtalen vedrører følsomme emner.

Eksempel: Diskutere personlige finansielle oplysninger højt på offentlige steder kan udsætte dig for risikoen for uautoriseret overvågning.

Vi vil hjælpe til at adfærdens er følgende...: Mens du venter på din tur i køen i supermarkedet, bliver du ringet op af din bank angående dine økonomiske oplysninger. Du flytter diskussionen til et mere privat sted for at undgå at dele følsomme oplysninger med andre, der kan lytte.

Hvorfor taler folk stadig vidt og bredt om følsomme ting i toget?

Spear Phishing

(smishing (SMS), vishing (tlf), phishing (mail))

Hvad det er: Spear phishing er en målrettet form for phishing, hvor angriberen skræddersyr angrebet til en specifik person eller organisation.

Eksempel: Modtagelse af en e-mail, der synes at komme fra en kollega med specifikke og personlige oplysninger, bør udløse forsigtighed.

Vi vil hjælpe til at adfærden er følgende...: Du modtager en e-mail, der angiveligt er fra din leder og beder om adgang til følsomme virksomhedsdokumenter. Du bemærker imidlertid nogle stavefejl og usædvanlige anmodninger, hvilket får dig til at kontakte IT-afdelingen for at bekræfte, om e-mailen er legitim.

Hvorfor er det stadig den mest udbredte metode?

IT derhjemme



Beskrivelse: Med mange medarbejdere, der arbejder eksternt, er sikkerheden af hjemmearbejdspladser afgørende. Dette inkluderer beskyttelse mod usikre netværk, opdaterede enheder og adgangskontrol.

Eksempel: Hjemmearbejdspladser er blevet mål for cyberangreb, og derfor er det vigtigt at højne sikkerheden her.

Vi vil hjælpe til atadfærdens er følgende...: Du ønsker kun at gøre brug af sikre netværk, og har derfor også 2 routere derhjemme - en til arbejde og en til privat. Før dette, havde du også ændret standardkoden på routeren.

Hvorfor forholder medarbejdere ikke sig til sikkerhed derhjemme?

Huske opdateringer

Hvad det er: Opdateringer til din computer inkluderer rettelser til sikkerhedshuller og forbedringer af systemets stabilitet.

Eksempel: Ignorering af vigtige systemopdateringer kan efterlade din enhed åben for malware-angreb, der udnytter kendte sårbarheder.

Vi vil hjælpe til at adfærdens følgende...: Når du lukker din computer ned for dagen, bemærker du en meddelelse om tilgængelige opdateringer. I stedet for at udskyde dem, vælger du at installere opdateringerne straks for at sikre, at din enhed forbliver beskyttet mod de seneste trusler.

Hvorfor er folk så dårlige til at huske opdateringer, på trods af påmindelser?

Private konti adskilt fra arbejde



Hvad det er: At adskille private og arbejdskonti bidrager til at bevare personlige oplysninger og sikre, at arbejdsrelaterede data forbliver sikre.

Eksempel: Brug af arbejdsmail til personlige online-tjenester kan øge risikoen for datalæk og kompromittere arbejdsrelaterede oplysninger.

Vi vil hjælpe til atadfærdens følgende...: Du arbejder hjemmefra og opretter separate mapper og konti på din computer til adskillelse af personlige og arbejdsrelaterede oplysninger. Dette hjælper med at bevare fortroligheden og organiseringen af dine data.

Hvorfor bruger folk stadig deres virksomhedsmail til private gøremål?

Passwords

Hvad det er: Adgangskoder er korte, ofte komplekse tegnserier, mens passphrases er længere sætningsfragmenter, begge bruges til at beskytte konti.

Eksempel: En stærk adgangskode kombinerer bogstaver, tal og specialetegn for at øge sikkerheden, f.eks. "P@ssw0rd_Str0ng!"

Vi vil hjælpe til at adfærdens er følgende...: Når du opretter en ny konto på en online butik, vælger du at bruge en stærk passphrase i stedet for en simpel adgangskode. Dette sikrer, at din konto er godt beskyttet mod uautoriseret adgang.

Hvorfor bruger de stadig de samme passwords til alle konti?

VPN

Des- og misinformation

Minimer digitale fodaftryk

Malicious Attachments

Lås skærmen

Ukorrekte eller usikre links

MFA

Samtaler i det offentlige rum

Spear Phishing

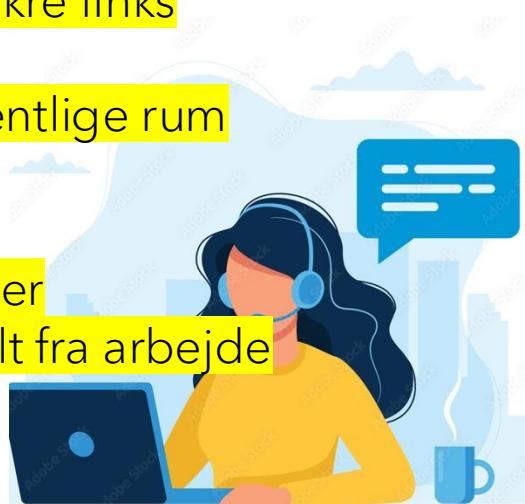
IT derhjemme

Huske opdateringer

Private konti adskilt fra arbejde

Passwords

Tailgating



Forlystelsesparken "WeHaveFun" med fokus på DK's vildeste rutchebaner...



Ilse, 62 år. Kundserviceleder, med adgang til hele kundedatabasen (årskort m.m.), hvem der ikke har betalt osv. Håndterer de fleste typer henvendelser

Ole, 58 år. Teknisk leder, med ansvar for de der servicerer forlystelser og adgang til centrale systemer for at kunne håndtere driftsforstyrrelser.

Mette 26 år. Leder med ansvar for den daglige drift i parken, ansvaret for 100 ung-arbejdere (sæsonansatte) og 20 fastansatte

Diskuter hvilke temaer der er mere aktuelle end andre for hver af de 3 medarbejdere, tal om scenarier, og hvad der er vigtigt når det handler om kommunikationsstrategi/formater ift at ændre adfærd. **Brug 10 min på hver persona.**