ERHVERVS SAMMENSLUTNINGEN

Cybersikkerhed, har din virksomhed fokus..

Secure Practice ip.dots

Agenda

- IP Dots/KAPI
- Indledning
- Secure Practice
- Cybersikkerhed Awareness Træning
- Anbefalinger
- Evt. spørgsmål

ERHVERVS SAMMENSLUTNINGEN

IP Dots

Synlighed • Sikkerhed • Kontrol

Secure Practice ip.dots

IP Dots

ERHVERVS SAMMENSLUTNINGEN

- Konsulentvirksomhed med fokus på administration og optimering af online synlighed, cybersikkerhed og brand kontrol.
- Virksomheden er grundlagt i 2016 og har kontor i Albertslund (København).
- Enorm fokus på personlig service, rådgivning og proaktivitet med Single-Point-of-Contact, dansk 24/7 support.
- Vi arbejder benhårdt på at udvikle tætte, langvarige og tillidsfulde relationer.
- Fleksibel og dynamisk forretningsmodel – vi tilpasser os og vores service set-up, til vores klienters unikke ønsker og behov.

DANSK ERHVERV

IT-BRANCHEN

SKI LEVERANDØR

Secure Practice ip.dots

Løsninger og services

ERHVERVS SAMMENSLUTNINGEN

Domain Name Management
- Registration
- Renewals
- Consolidation
- Recovery / Acquisition
- Strategy development

Domain Name Monitor
- Baseline report
- Monitoring
- Frequent follow-up & consulting

Premium DNS
- Cloudflare
- Microsoft Azure
- Amazon Web Services (AWS)
- NoteSecure
- Anycast, DDoS Protection, DNSSEC

Domin Name Blocking
- Global Block
- Adult Block
- DPML Block

Certificates
- SSL/TLS
- Code Signing
- S/MIME
- VMC
- PKI

E-mail Security
- DMARC Compliance service
- Email Defence (e-mail scan)
- DNS Defence (DNS scan)
- Cloudflare/Azure/AWS

Cybersecurity Training
- Employee awarenes training
- Simulated phishing attack
- Integrated email risk system (Office365)

Consultant services
- Strategic consulting
- Domain name strategy
- Brand Analysis
- Technical consulting
- Security consulting

Trademark Administration
- Registration
- Renewal
- Enforcement
- Audit
- Strategy development

Legal Consulting
- Assessment of opportunities and rights
- Help with formal complaints and legal proceedings

Cloudflare Solutions
- Secure Access Service Edge (SASE) & Security Service Edge (SSE)
- Advanced application security and performance
- Network Services - secure, connect, and optimize
- Developer Services - innovate faster and more securely

Secure Practice ip.dots

KAPI

Cyber- og Behandlings-sikkerhed

KAPI

Video2Learn

IT-sikkerhed

Computervirus

1. Hvad er en computervirus
2. Beskyttelse mod computervirus

Sikkerhed

1. Hvorfor er adgangskoder vigtige
2. Netværksforbindelse - hjemmearbejde

Phising

1. Phishing
2. Spear Phishing, whaling, smishing, vishing
3. Gode råd til at undgå phishing

Sikkerhed diverse

1. 1. Hvad er et databrud
2. Sikker mail
3. Spam

Cookies

1. Cookies generalt
2. Cookies GDPR
3. 3.parts cookies

Kontakt

Pia Larsen

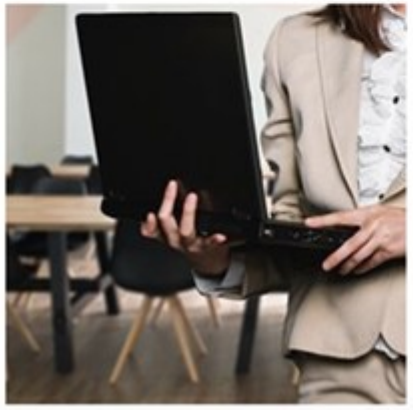
psl@kapi.dk
28951131

KAPI

GDPR

Implementering

Opstart og gennemgang af procedure-beskrivelser (artikel 30) gennemgås, hvis den findes og ellers udarbejdes den.
Databehandleraftaler gennemgås og risikovurderes.
Opstart og opsætning af GDPR Awareness-pakke – kurser til alle faggrupper.
Gennemgang/udarbejdelse af procedurebeskrivelser og politikker
Opsætning af kontroller og årshjul
Opsætning af Risiko-analyse for samtlige databehandlere
Beredskabsplan
Opsætning af hændelseslog til brug ved eventuelle databrud m.v.



Drift

Årlig stikprøvekontrol med efterfølgende udarbejdelse af direktions-/bestyrelsesrapport og udtalelse.
Kontrol af databehandlere minimum 1 gang årligt – afhængig af risikoprofil
Årlig awareness af medarbejdere
Besvarelse af forespørgsler fra fx samarbejdspartnere og leverandører, datatilsynet
Gennemgang af hændelseslog

Indledning

- De fleste virksomheder investerer rigtigt mange penge i at gøre deres brands stærke og letgenkendelige, men typisk bliver der desværre ikke brugt mange penge på, at beskytte denne investering.
- Det er svært at styre hvad andre gør, så det nemmeste er at sørge for at ens eget brand ikke bliver involveret i en uheldig situation. Tag kontrol over jeres brand og beskyt det.
- Vi ser tit at organisationer desværre ikke proaktivt får sikret domæner, DNS og e-mailservere der matcher deres brands, der hvor det er relevant, hvilket betyder at de mister kontrollen over hvad deres brands bliver brugt til og associeret med. Lige så ofte oplever vi desværre at cybersikkerhed slet ikke er inkluderet i overvejelserne omkring organisationernes eksterne cloud og API løsninger.
- Man kan aldrig sikre sig 100%, men man kan minimere risikoen for at ens brand bliver misbrugt eller bliver involveret i en scam eller et cyberangreb.
- En god firewall er ikke længere nok! I dag kommer op til 90% af alle målrettede cyberangreb ind i en virksomhed via emails. Alligevel oplever vi at de fleste virksomheder udelukkende har fokus på beskyttelse ift. cyberangreb fra firewall og indad, men stort set ingen fokus har på hvordan problemet opstår – eller kommer forbi deres firewall.

Den globale konsekvens

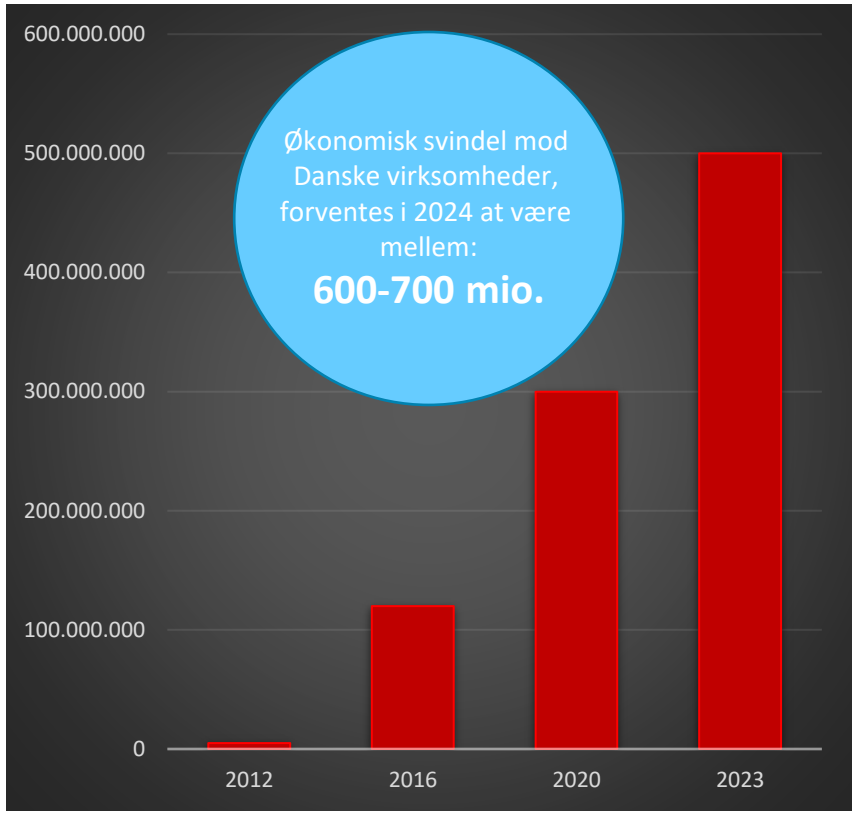
- I 2021 skabte konsekvensen af cyberangreb og -kriminalitet skader for i alt 6 billioner dollars på verdensplan[1]. Hvis vi tænker på dette tal som et land, ville det være verdens tredjestørste økonomi efter USA og Kina.
- Antallet af cyberangreb vokser eksplosivt år for år. Ifølge diverse undersøgelser har minimum 40%, og helt op til 90%, af adspurgte organisationer oplevet et cyberangreb. Det er derfor ikke længere et spørgsmål om man bliver angrebet, men et spørgsmål om hvornår det vil ske. Siden COVID pandemien ramte, har FBI rapporteret stigninger på op imod 300% i cyberkriminalitet[2].
- Aktuelle tendenser som cloud-teknologi, fjernarbejde og enheder forbundet med 5G-teknologien forårsager mere skade end nogensinde før.
- Forventningen for 2024 er at det når op på at skader relateret til cyberkriminalitet har en effekt på 10,5 billioner dollars årligt[3].

Kilder:
1. Morgen, S. Cybercrime to Cost the World $10.5 Trillion Annually by 2020, Cybersecurity Ventures, 12 November 2020.
2. Walter, J. COVID-19 news: FBI Reports 300% Increase in Reported Cybercrimes, IMC Grupo, 2 May 2020.
3. Morgen, S. Cybercrime to Cost the World $10.5 Trillion Annually by 2020

Fakta

Danske virksomheder rammes i stigende grad af bedrageriforsøg via email

- Fra 2012 til 2023 vækstede svindel via email voldsomt, og konsekvensen for de danske virksomheder var et tab der gik fra 5 mio. kr. til 500 mio. kr. om året[1, 2, 3.]
- Mere end hver 3. adspurgte virksomhed har oplevet forsøg på email svindel[4]
- I 2023 blev mere end hver anden virksomhed ramt af et eller flere cyberangreb[5]
- En undersøgelse viser at 21% af de undersøgte DNS records for subdomæner, peger på indhold det der ikke resolver, hvilket gør subdomæne hijacking muligt[6]
- Undersøgelsen viste også at 79% af de registrerede domæner, der til forveksling ligner Global2000 Brands (også kaldet homoglyphs), ejes af tredjeparter, heraf bruges 40% til at udsende mails[6]



Kilder:

I) Kriminalitet i en digitaliseret verden Identitetstyveri og bedrageri på internettet, Peter Kruize, Københavns Universitet, Maj 2013
2) Falske direktører har snydt danske virksomheder for 200 millioner kroner på et år (berlingske.dk)
3) LCIK's Årsrapport 2020: LCIK årsrapport 2020 (politi.dk)
4) Nu er cyberkriminaliteten blevet personlig - IT-Branchen (itb.dk) cybercrime-survey-2020.pdf (pwc.dk)
5) cybercrime-survey-2023.pdf (pwc.dk)
6) Corporation Service Company® - 2023 DOMAIN SECURITY REPORT

GDPR og Cybersikkerhed (NIS2)

IT-sikkerhed (overordnet begreb)
Handler om beskyttelse af information, systemer og netværk mod uautoriseret adgang, ændring og ødelæggelse
Omfatter både cybersikkerhed og fysisk sikkerhed (f.eks. adgangskontrol til serverrum).

Cybersikkerhed (del af IT-sikkerhed)
Fokus på digitale trusler som hacking, malware, phishing og DDoS-angreb.
Inkluderer tekniske løsninger som firewalls, kryptering og netværksovervågning.

Behandlingssikkerhed (del af GDPR og databeskyttelse)
Sikrer, at persondata håndteres korrekt og sikkert ifølge GDPR.
Handler om både tekniske og organisatoriske foranstaltninger (adgangsstyring, logging, dataminimering osv.).

KAPI

GDPR og Cybersikkerhed

GDPR og Cybersikkerhed går hånd i hånd.

- GDPR fastsætter **hvad** der skal beskyttes og **hvorfor**
- IT- og cybersikkerhed handler om **hvordan** beskyttelsen implementeres i praksis.

En stærk IT og Cybersikkerhedsstrategi er afgørende for at overholde GDPR og undgå både juridiske og operationelle risici.

KAPI

GDPR og Cybersikkerhed

Artikel 32 i GDPR kræver:

At dataansvarlige og databehandlere implementerer passende tekniske og organisatoriske sikkerhedsforanstaltninger for at beskytte personoplysninger mod uautoriseret adgang, tab, ændring eller ødelæggelse.

Disse sikkerhedsforanstaltninger inkluderer:

•Kryptering af data
•Adgangskontrol og autorisation
•Overvågning og logning af systemadgang
•Sikkerhedstests og risikovurderinger
•Backup og gendannelsesprocedurer
•Undervisning af medarbejdere
•Løbende kontrol

KAPI

GDPR og Cybersikkerhed

Cybersikkerhed som middel til GDPR-overholdelse:

- **Forebyggelse af databrud**: Cybersikkerhed reducerer risikoen for databrud.
- **Beskyttelse af fortrolighed, integritet og tilgængelighed**: GDPR kræver, at virksomheder beskytter personoplysninger mod cybertrusler som hacking, malware og phishing.
- **Dokumentation og sporbarhed**: Cybersikkerhedsværktøjer som logning og revisionsspor hjælper med at dokumentere compliance og muliggør sporing af potentielle brud

KAPI

GDPR og Cybersikkerhed

Konsekvenser ved manglende cybersikkerhed:

•Virksomheder, der ikke lever op til GDPR's sikkerhedskrav, risikerer **bøder på op til 4% af den globale omsætning eller 20 millioner euro**, afhængigt af hvad der er højest.

•Et sikkerhedsbrud kan føre til tab af kundetillid, juridiske konsekvenser og økonomiske tab

GDPR og Cybersikkerhed

- **Best Practices for at kombinere Cybersikkerhed og GDPR**
- **Dataminimering**: Indsaml kun de nødvendige personoplysninger.
- **Kryptering**: Beskyt data både under opbevaring og transmission.
- **Stærk adgangskontrol**: Implementér multi-faktor-autentifikation (MFA) og rollebaseret adgang.
- **Løbende sikkerhedsopdateringer**: Patch systemer for at lukke sårbarheder.
- **Bevidsthedstræning**: Uddan medarbejdere i at genkende cybertrusler.
- **Incident Response Plan**: Hav en klar plan for håndtering af sikkerhedsbrud

KAPI

Konsekvenser

- Brand værdi
- Tillid
- Online trafik
- Tid
- Omsætning
- Fortjeneste

ERHVERVS SAMMENSLUTNINGEN

Ansvar for sikkerheden

Hvem har ansvaret og i hvilken afdelingen ligger det?

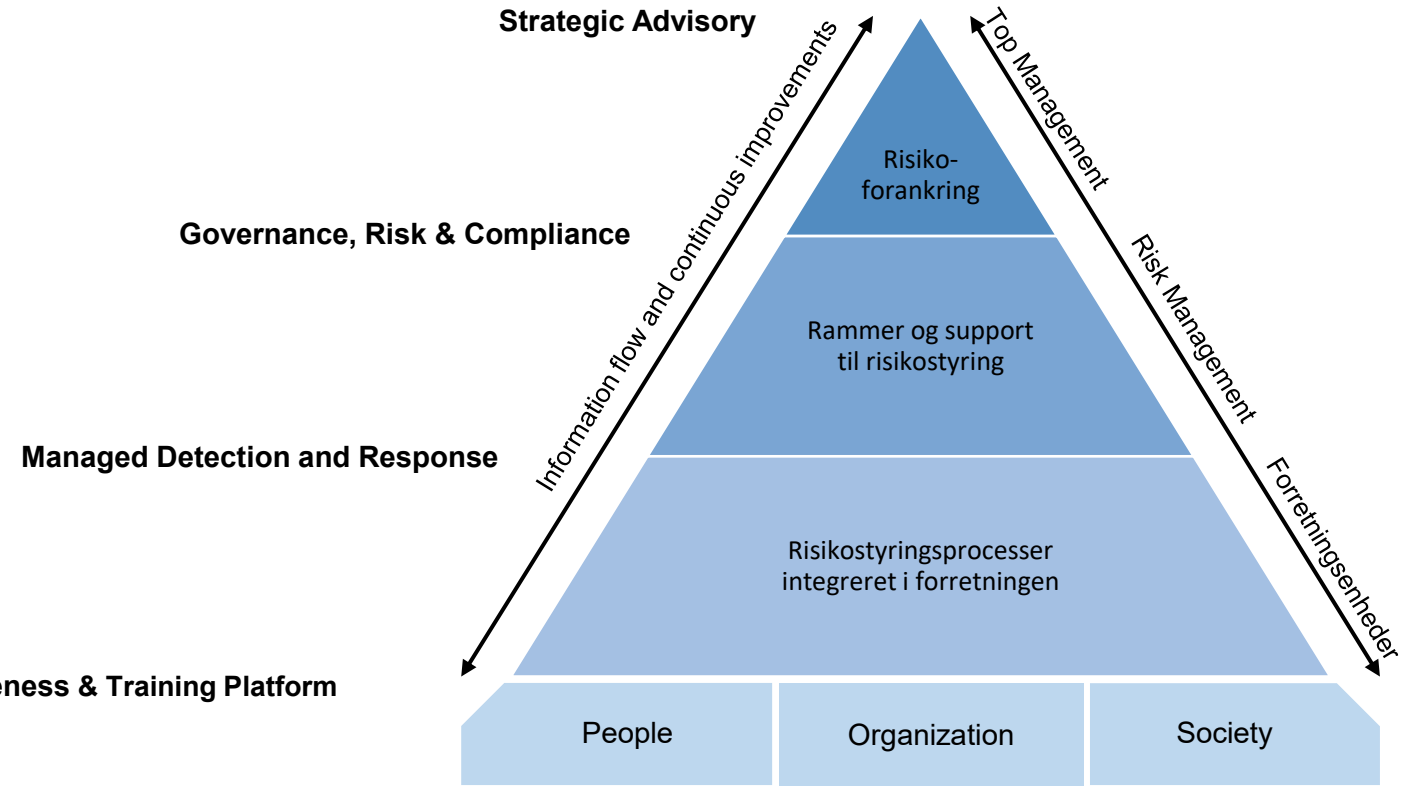
Secure Practice ip.dots

Risikostyring

ERHVERVS SAMMENSLUTNINGEN

Secure Practice funktioner:

- Cyber Exercises
- MailRisk
- Simulated Phishing
- Gamified E-learning
- Human Risk Metrics



Secure Practice ip.dots

Skab en sikkerhedskultur

ERHVERVS SAMMENSLUTNINGEN

ENGAGE

MailRisk analysis and response

INFLUENCE

Simulated phishing and e-learning

CULTIVATE

Metrics and measures for change

Secure Practice ip.dots

ERHVERVS SAMMENSLUTNINGEN

Secure Practice

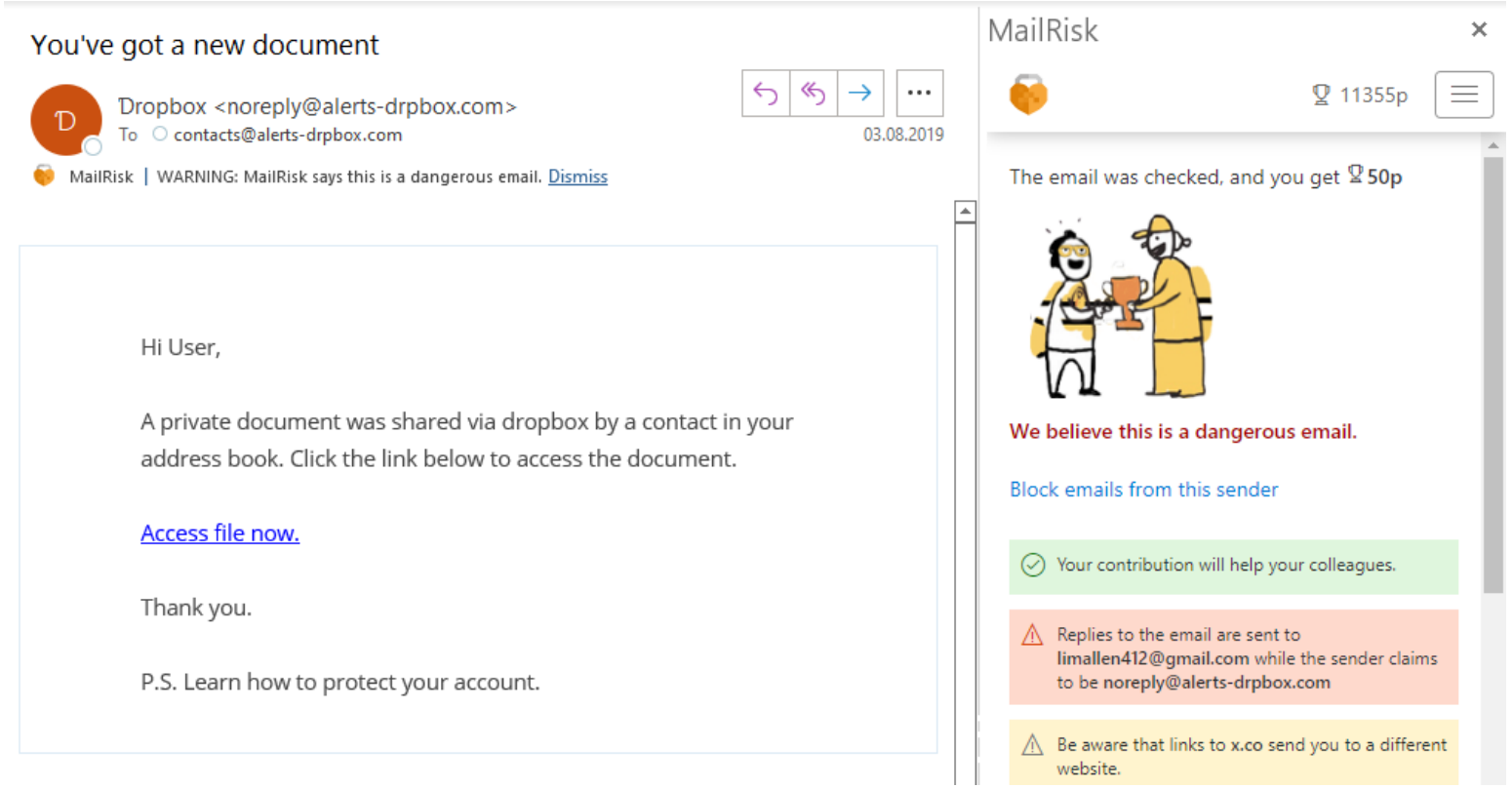
Cybersikkerhed Awareness Træning

Secure Practice ip.dots

MailRisk

ERHVERVS SAMMENSLUTNINGEN

Altid hjælp med mistænkelige e-mails

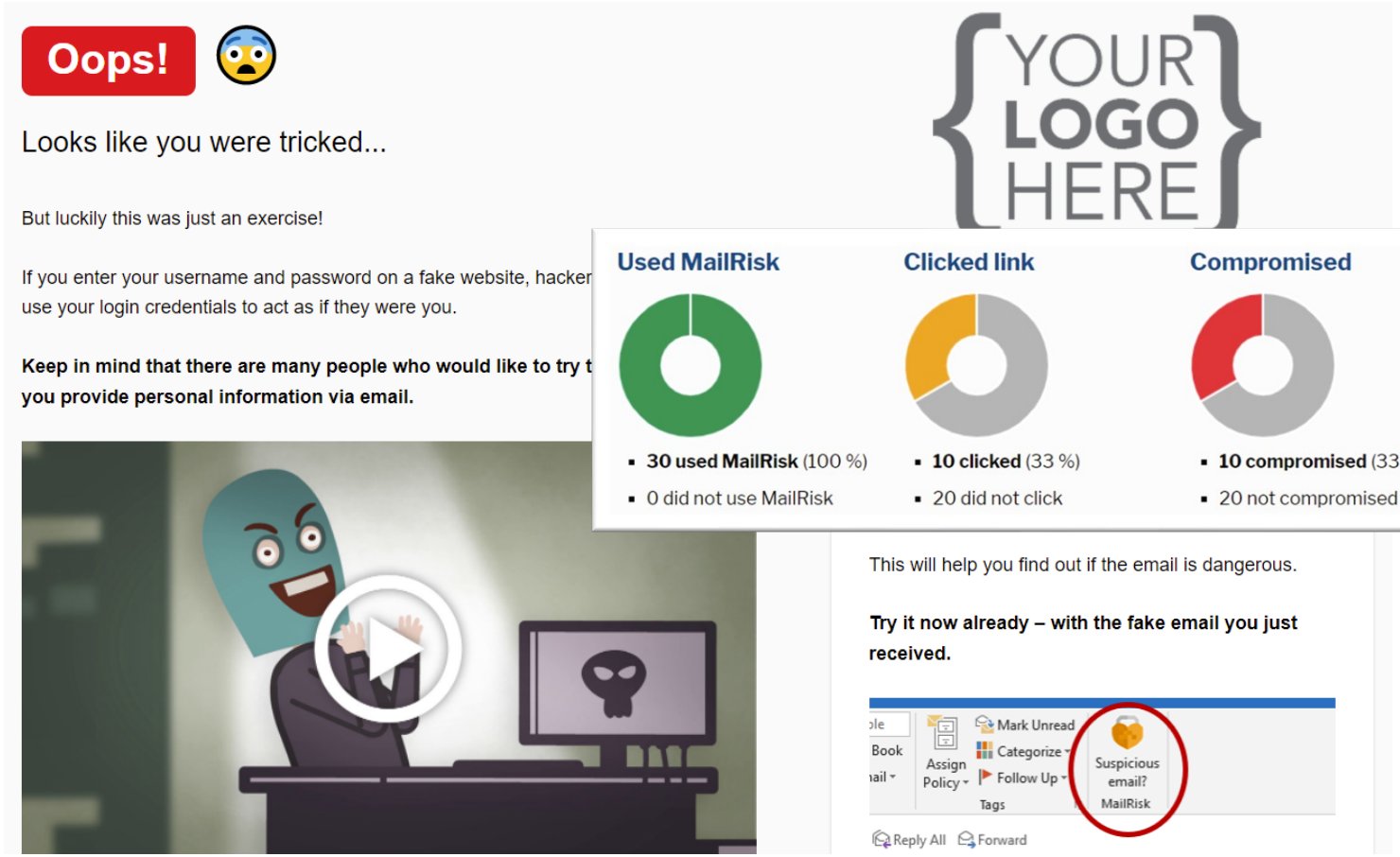


Secure Practice ip.dots

Simuleret phishing

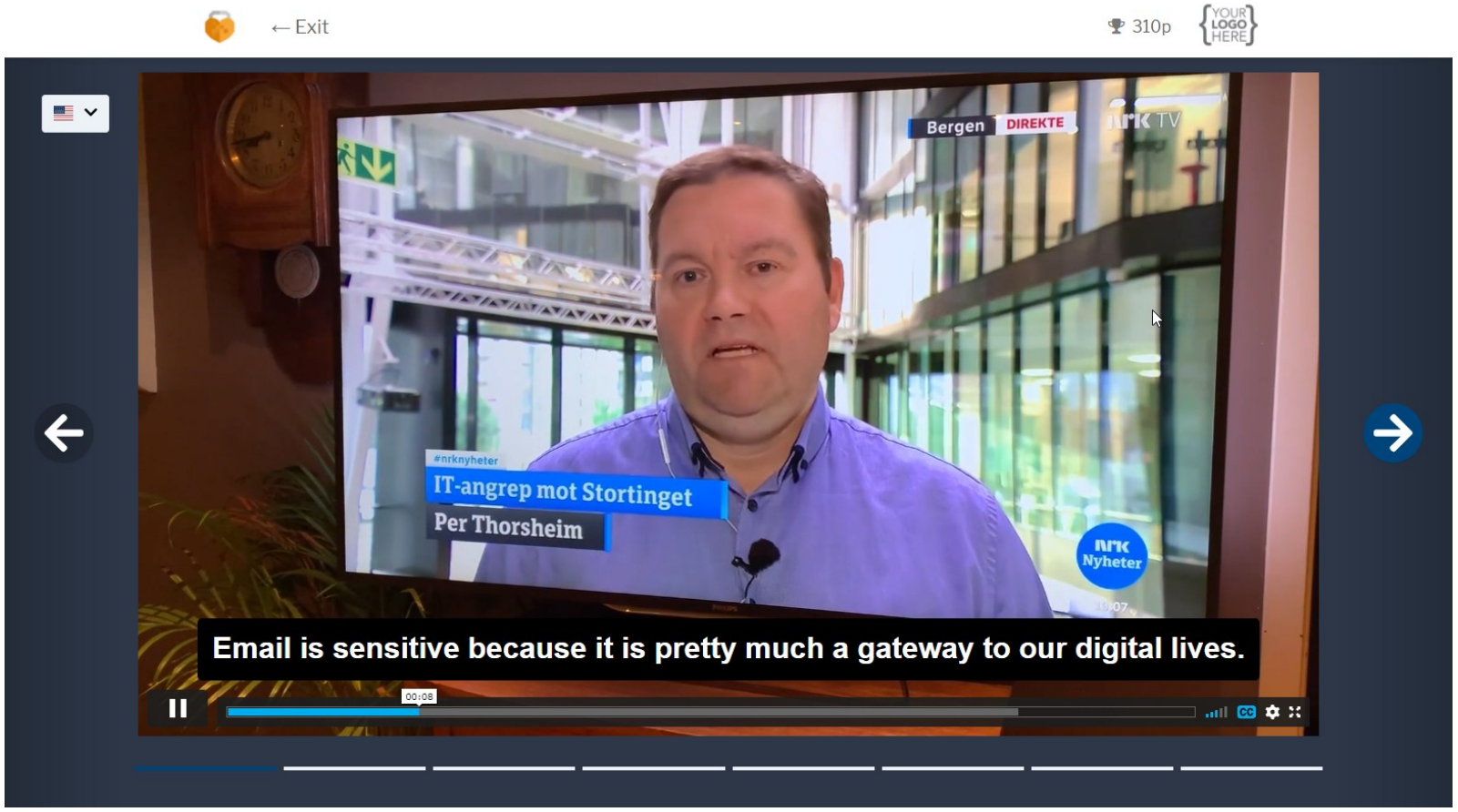
ERHVERVS SAMMENSLUTNINGEN

Simulerings kanaler:
- e-mail
- SMS
- Tale



Secure Practice ip.dots

Gamificeret e-læring



ERHVERVS SAMMENSLUTNINGEN

Anbefalinger

20 gode råd du kan tage med hjem

Secure Practice ip.dots

21 Gode Råd til Cybersikkerhed

ERHVERVS SAMMENSLUTNINGEN

- **Brug Stærke Adgangskoder** – Anvend komplekse og unikke adgangskoder samt en password manager.
- **Aktivér Multi-faktor Autentifikation (MFA)** – Øger sikkerheden ved login.
- **Adgangsbegrænsning** – Giv kun adgang til data og systemer efter behov.
- **Begræns Administratorrettigheder** – Kun få brugere bør have udvidede rettigheder.
- **Administrér Tredjepartsadgange** – Vurder sikkerheden hos samarbejdspartnere.
- **Hold Software Opdateret** – Installer sikkerhedsopdateringer løbende.
- **Sikkerhedskopiering** – Tag regelmæssige backups og test gendannelse.
- **Brug Firewall og Antivirus** – Beskyt netværket mod trusler.
- **Sikre Netværksforbindelser** – Brug VPN ved eksterne forbindelser.
- **Sikre Mobile Enheder** – Brug MDM-løsninger (Mobile Device Management).
- **Begræns Brugen af USB-enheder** – Reducér risikoen for malware.
- **Brug Sikre Cloud-løsninger** – Vælg leverandører med stærke sikkerhedsforanstaltninger.
- **Kryptering af Data** – Beskyt følsomme oplysninger mod tyveri (certifikater).
- **Overvåg Systemer for Uregelmæssigheder** – Implementér logning og analyseværktøjer.
- **Gennemfør Penetrationstests** – Test jævnligt virksomhedens sikkerhedsniveau.
- **Sikre de eksterne faktorer** – Beskyt dine domæne/brand, DNS og e-mails
- **Indfør Incident Response Plan** – Hav en beredskabsplan klar ved sikkerhedsbrud.
- **Opdater Sikkerhedspolitikker** – Sørg for klare retningslinjer for IT-sikkerhed.
- **Oplær Medarbejdere** – Gennemfør løbende cybersikkerhedstræning.
- **Beskyttelse mod Phishing** – Vær skeptisk over for mistænkelige e-mails og links.
- **Overhold Lovgivning og Standarder** – Følg GDPR, NIS2 og andre relevante standarder.

Ved at implementere disse 21 råd styrker din virksomhed sin modstandsdygtighed over for cybertrusler.

Secure Practice ip.dots

Cybersikkerhed Awarenesstræning

ERHVERVS SAMMENSLUTNINGEN

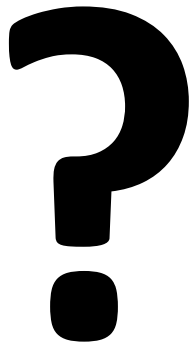
- **Engager jeres medarbejdere med virkelige simulationer:** Gennem simuleret phishing og andre interaktive øvelser oplever medarbejderne realistiske scenarier, hvilket forbedrer deres evne til at genkende og reagere på faktiske trusler.
- **Personlige læringsstier for hver enkel medarbejder:** Hver medarbejder modtager skræddersyet træning, der er tilpasset deres rolle og nuværende vidensniveau, hvilket sikrer den mest relevante og effektive læringsoplevelse.
- **Leg med gamification og skab en positiv styrkelse:** Vores platform bruger gamification-teknikker til at gøre læring sjovt og belønnende, hvilket fremmer en sikkerhedsorienteret tankegang.
- **Kontinuerlig forbedring af medarbejderne:** Vi leverer metrikker og analyser til at spore fremskridt og identificere forbedringsområder, hvilket sikrer, at dine sikkerhedspraksisser udvikler sig i takt med trusselslandskabet.

Vi vil gerne tilbyde en præsentation af platformen og en gratis 30 dage prøveperiode

Secure Practice ip.dots

Spørgsmål

ERHVERVS SAMMENSLUTNINGEN



Secure Practice ip.dots