DATASÄKERHET FÖR SMÅFÖRETAG

6.3.2025

dg CREATIVE

dg CREATIVE

Joel Sjöblom

VD
DG Creative

DAGENS AGENDA

1. Välkommen och intro
2. Vad är datasäkerhet och varför berörs även mindre organisationer
3. Varför behöver vi prata om datasäkerhet
4. Vad sker i världen, och i vår närområdesgivning
5. Hur kommunicerar vi idag, och med vilka hjälpmedel?
6. Social Engineering
7. Grundläggande principer kring datasäkerhet
8. Smart Technology

VAD ÄR DATASÄKERHET

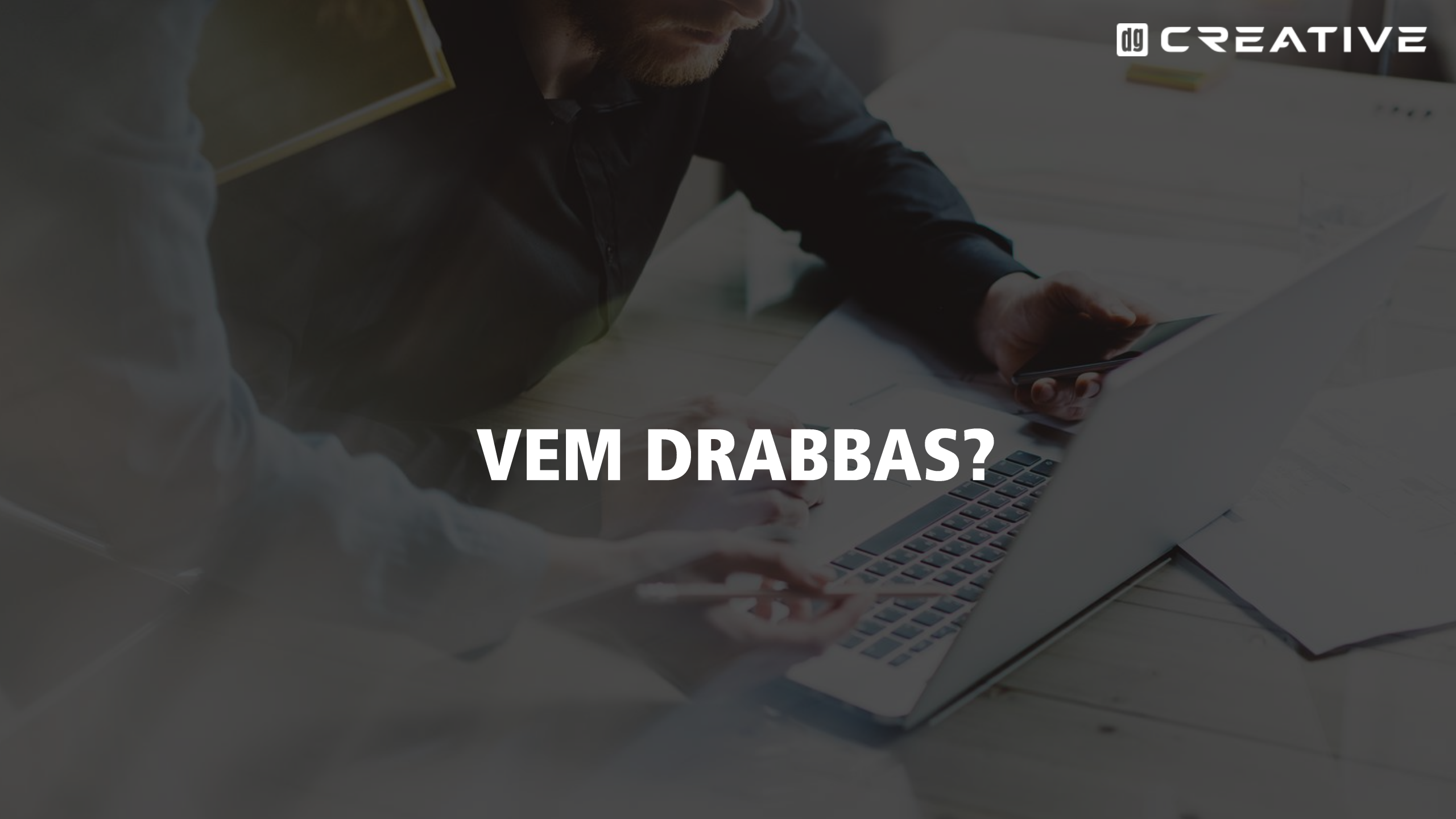
VARFÖR DISKUTERA DATASÄKERHET

DIGITALISERINGEN

2000	Bredband, snabbare internet
2004	Sociala Medier
2007	Smartphones
2009	Kryptovalutor (t.ex. Bitcoin)
2012	Molntjänster (Google Drive, AWS)
2014	IoT – Uppkopplade enheter
2019	5G-nätverk
2022	Generativ AI

PANDEMIN

DAGENS GEOPOLITISKA SITUATIONEN


dg CREATIVE
VEM DRABBAS?

Helsingfors stad misstänker dataintrång från Ryssland

Publicerad 01.05.2024 22:15. Uppdaterad 01.05.2024 22:27.

Helsingfors mål för massivt dataintrång – upp till 80 000 elevers personuppgifter kan ha läckt

Publicerad 13.05.2024 15:14. Uppdaterad 14.05.2024 15:01.

KRP: Helsingin tietomurto on Suomen kaikkien aikojen suurin – näin tutkinta etenee nyt

Kiristyksestä tai tietojen päätymisestä pimeään verkkoon ei ole tietoa.

38 ARTIKLAR sedan 20 januari

11 februari

Efter hackerattacken i Vellinge: Journaler spårlöst borta
Många patientuppgifter kommer inte att gå att återställa

31 januari

IT-problemen lösta på regionen – avvecklar stabsläge
Efter attacken mot Tietoevry • Kunde inte skriva ut patienter

28 januari

Experten om IT-attacken mot regionen: ”Alltid allvarligt”
Namn och hälsodata kan ha läckt • Så kan du som patient agera

25 januari

Fyra regioner i stabsläge efter hackerattack

24 januari

Personuppgifter kan ha läckt från Region Västerbotten
Anmäler och utreder händelsen

Eskilstuna kommun utsatt för misstänkt it-angrepp
Upptäcktes under torsdagsförmiddagen

Sametinget en av de hackade myndigheterna
”Kan inte läsa lönespecifikationen”

Göteborgsteatrarnas hemsida ligger nere: ”It-attack”
Går att köpa biljetter • Del av Akiras it-attack

23 januari

Efter hackerattacken: Problemen värre

COOP-KEDJAN


Tillfälligt stängt!
Vi har råkat ut för en stor IT-störning och våra system fungerar inte.
Problemet drabbar tyvärr även andra tjänster i butiken, eftersom vi måste hålla helt stängd.
Vi beklagar att du som kund drabbas.
Plötsligt händer det!

20.12.2024

VALION JA MAIDONHANKINTAOSUUS-KUNTIEN HENKILÖSTÖN TIETOIHIN KOHDISTUNUT TIETOTURVAHYÖKKÄYS

Ransomware Paralyzes a German Hospital; Patient Dies due to Delayed Aid

By **CISOMAG** - September 23, 2020

SHARE Facebook Twitter G+

The Register

Save the Children hit by ransomware, 7TB stolen

A new low, even for these lowlifes

Aleksanteri Kivimäki döms till 6 år och 3 månaders fängelse i Vastaamofallet

Den åtalade Aleksanteri Kivimäki döms till fängelsestraff i Vastaamofallet. Tingsrätten förkastade inga av åtalen.

Den misstänkte i Vastaamofallet, Aleksanteri Kivimäki, blev i februari frisläppt från häktet i Vanda, men häktades på nytt igen då han inte längre dök upp i rätten. Bild: Henrietta Hassinen / Yle

EVA LAMPPU

30.4.2024 14:08 · Uppdaterad 30.4.2024 17:11

VARFÖR SMÅFÖRETAG ÄR I RISKZONEN

- Mindre IT-skydd jämfört med större bolag.
- Ofta brist på utbildning kring cybersäkerhet.
- Hackare ser småföretag som en "lätt väg in" till större mål (supply chain-attacker).

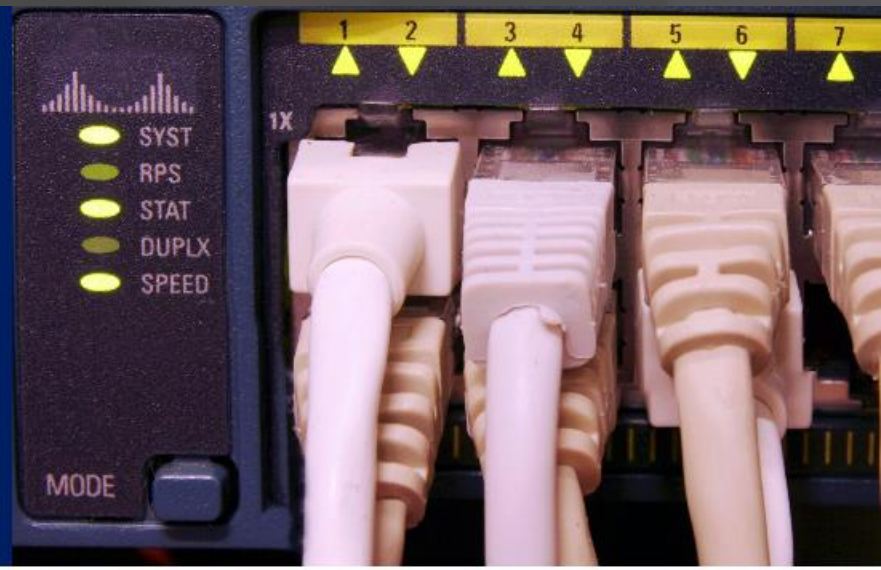
NYHEDSARTIKEL

MANGE DANSKE VIRKSOMHEDER ER RAMT AF HACKERANGREB: "DER ER INGEN VIRKSOMHED TILBAGE"

SKREVET DEN 23/08/2023

MAGNUS BANG

BANG@RADIO4.DK



De danske hostingselskaber Azerocloud og Cloudnordic er ramt af hackerangreb. Det har resulteret i, at flere hundrede danske virksomheder ikke længere kan tilgå deres data.

Cyberangrebet gør lige nu livet rigtig surt for de mange mellemstore og mindre virksomheder. For angrebet har betydet, at de har mistet deres hjemmesider, mailindbakker, og alt det de har gemt i deres såkaldte cloud.

Martin Haslund Johansson, direktør for hostingselskaberne Azerocloud og Cloudnordic, beklager situationen meget.

"Det her berører mig meget – jeg er rasende ked af det", lyder ordene fra direktøren.

Azerocloud og Cloudnordic er såkaldte hosting selskaber, som primært varetager deres kunders data. Derfor er det ikke kun disse to selskaber,

Inrikes Säkerhet

Fortums vd till Reuters: Misstänkta drönare och okända personer har rört sig vid anläggningarna

Bolaget har också utsatts för cyberattacker dagligen, rapporterar nyhetsbyrån Reuters.

Drönare och okända personer har vid flera tillfällen under det senaste året rört sig vid elbolaget Fortums anläggningar. Det uppger Fortums vd **Markus Rauramo** till nyhetsbyrån Reuters.

Bolaget ska också ha utsatts för överbelastningsattacker dagligen.

”Det har skett olika slags cyberattacker, eller försök till cybersäkerhetsintrång, dagligen och mindre frekvent har drönare och olika typer av misstänkt aktivitet upptäckts vid våra anläggnignar”, säger Rauramo till Reuters.

Rauramo säger att Fortum tagit i bruk omfattande säkerhetsåtgärder såsom reservsystem, skärpt kontroll gällande tillträde, privata säkerhetstjänster och övningar för att förebygga cyberattacker.

Svenska Yle,
10.10.2024

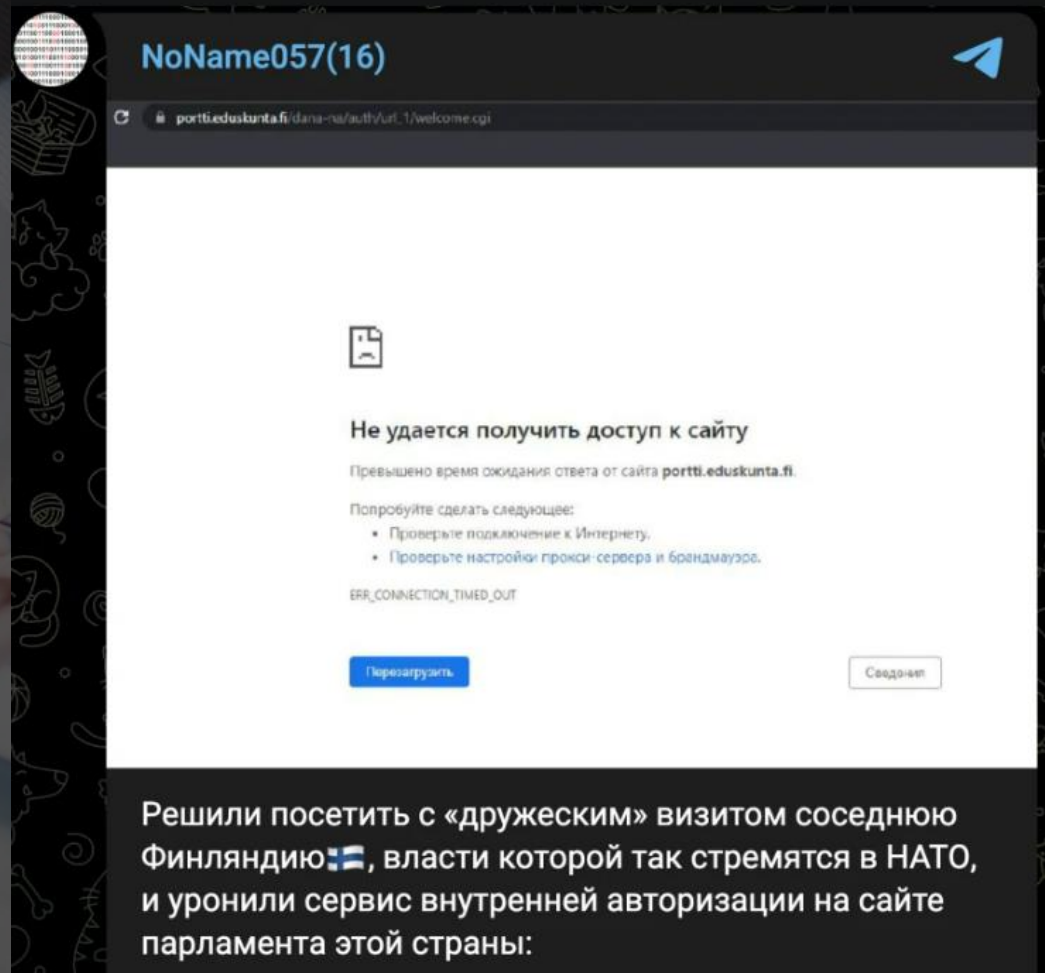
Riksdagens webbplats utsattes för rysk hackerattack – en av de mest kända hackergrupperna under kriget i Ukraina, säger expert

Från 2022 Publicerad 09.08.2022 17:21. Uppdaterad 10.08.2022 10:35.

Riksdagens webbplats blev på tisdagseftermiddagen utsatt för en överbelastningsattack. Sidan laddade tidvis väldigt långsamt och tidvis inte alls. En rysk känd hackergrupp tog på sig attacken.

Enligt Yles uppgifter har en rysk hackergrupp vid namn NoName057(16) meddelat på Telegram att de ligger bakom attacken.

"Vi bestämde oss för att göra ett "vänligt" besök i grannlandet Finland vars myndigheter blivit så angelägna om att gå med i Nato", skriver hackergruppen på kanalen, som motiv.




dg CREATIVE
HUR KOMMUNICERAR VI IDAG


dg CREATIVE
SOCIAL
ENGINEERING

yle Svenska Yle Arenan Ämnen Meny

ÖSTERBOTTEN

Österbotten Meny

Bedrägeriförsök mot Vasa Andelsbanks kunder har ökat

Publicerad 07.09.2023 11:06.

Chanette Härus

Dela

Under sommaren har bedrägeriförsök mot Vasa Andelsbanks kunder ökat.

Brottslingarna har slumpmässigt skickat meddelanden eller ringt offret och uppmanat dem överföra sina pengar till ett så kallat säkerhetskonto. I en del meddelanden har det också bland annat kunna stå att kunden måste kontrollera en betalning som gjorts med kundens bankkort eller att någon försökt göra en girering.

I flera meddelanden har det funnits en falsk länk som liknat Andelsbankens webbadress men som har haft skillnader i stavningen. Länken har lett till en sida som påmint om Andelsbankens men där det fiskas efter kundens bankkoder och kortuppgifter.

Vasa Andelsbanks riskhanteringsdirektör Christian Oikkonen påminner om att banken aldrig sänder kunder meddelanden som innehåller en länk till nätbankens inloggningssida. Banken ber heller aldrig om uppgifter om koder eller kort med ett meddelande eller per telefon.

Om en kund misstänker att hens koder har hamnat i fel händer är det bäst att genast spärra koderna.

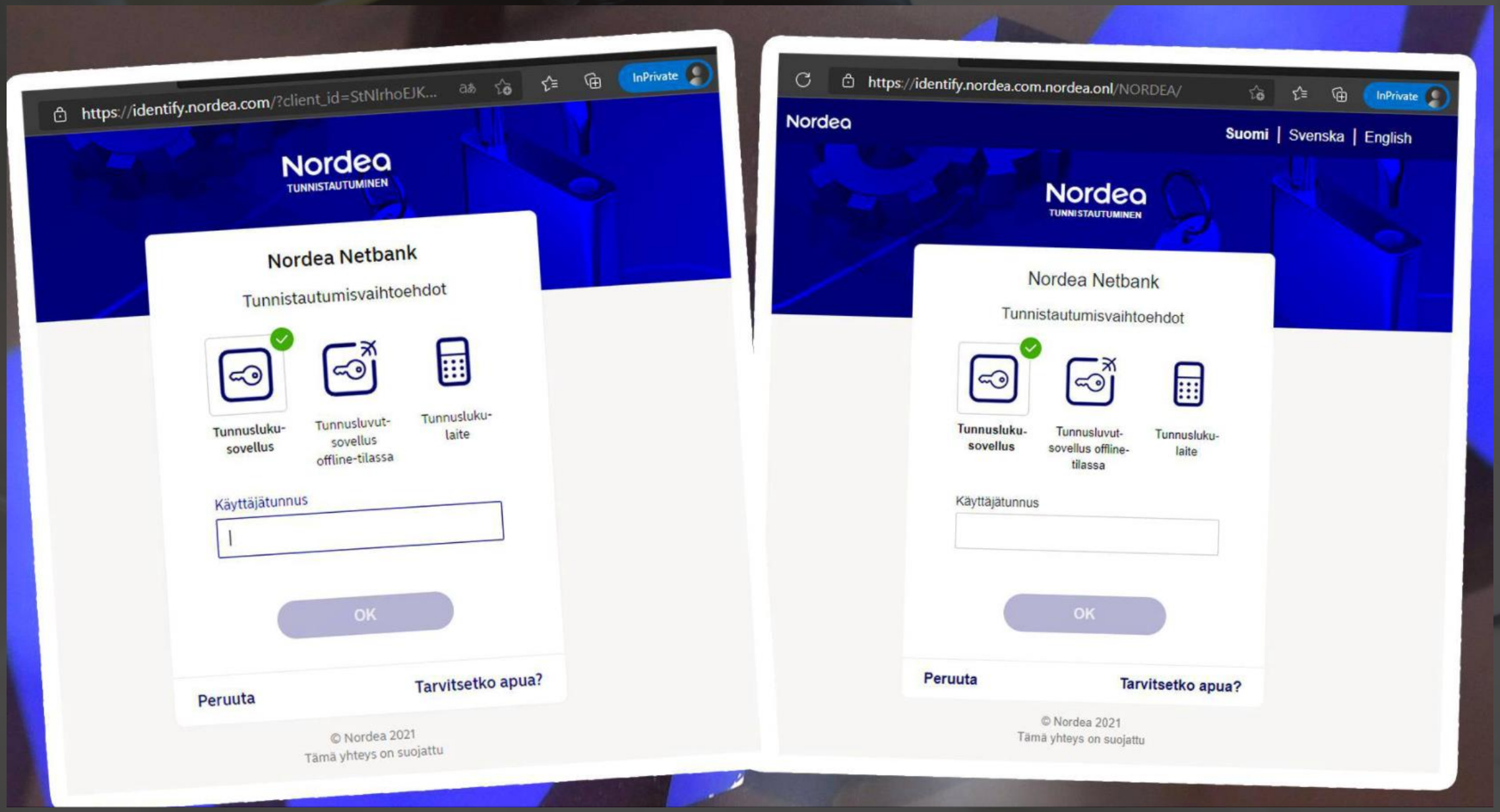
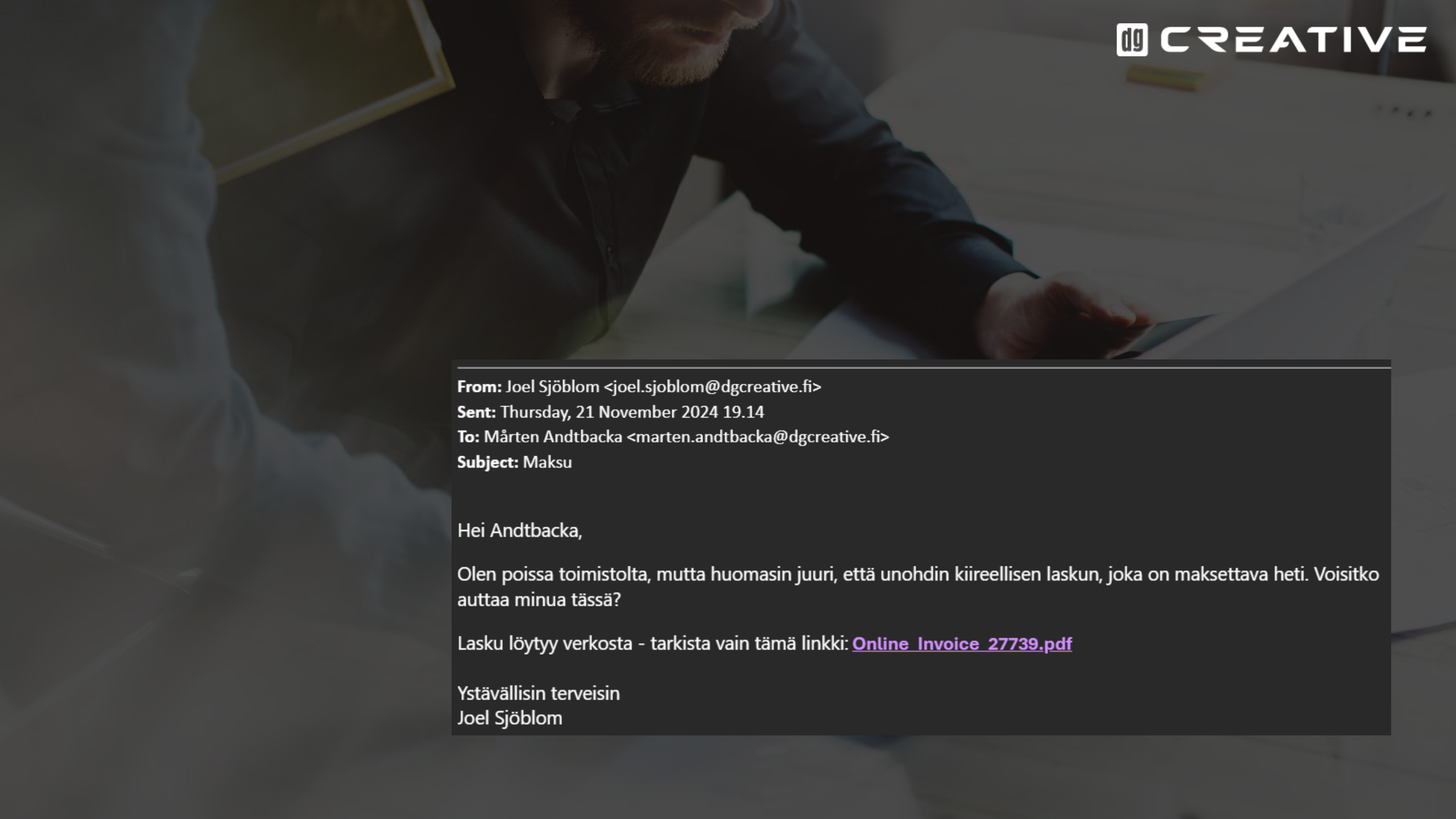

https://identify.nordea.com/?client_id=StNIrhoEJK...
InPrivate
Nordea
TUNNISTAUTUMINEN
Nordea Netbank
Tunnistautumisvaihtoehdot
Tunnusluku-sovellus
Tunnusluvut-sovellus offline-tilassa
Tunnusluku-laite
Käyttäjätunnus
OK
Peruuta
Tarvitsetko apua?
© Nordea 2021
Tämä yhteys on suojattu
https://identify.nordea.com.nordea.onl/NORDEA/
InPrivate
Nordea
Suomi | Svenska | English
Nordea
TUNNISTAUTUMINEN
Nordea Netbank
Tunnistautumisvaihtoehdot
Tunnusluku-sovellus
Tunnusluvut-sovellus offline-tilassa
Tunnusluku-laite
Käyttäjätunnus
OK
Peruuta
Tarvitsetko apua?
© Nordea 2021
Tämä yhteys on suojattu

Bild: Cybersäkerhetscentret



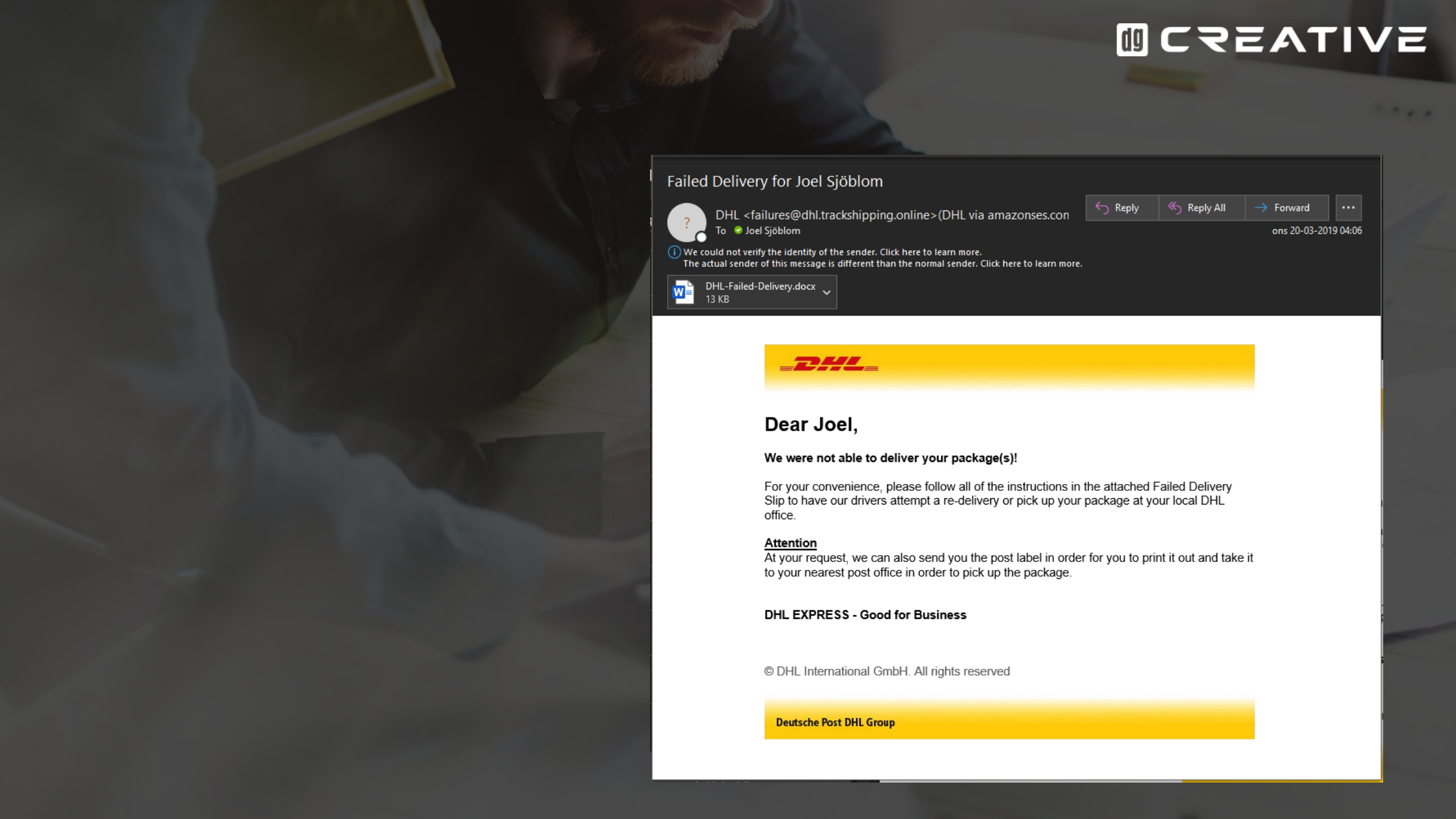
From: Joel Sjöblom <joel.sjoblom@dgcreative.fi>
Sent: Thursday, 21 November 2024 19.14
To: Mårten Andtbacka <marten.andtbacka@dgcreative.fi>
Subject: Maksu

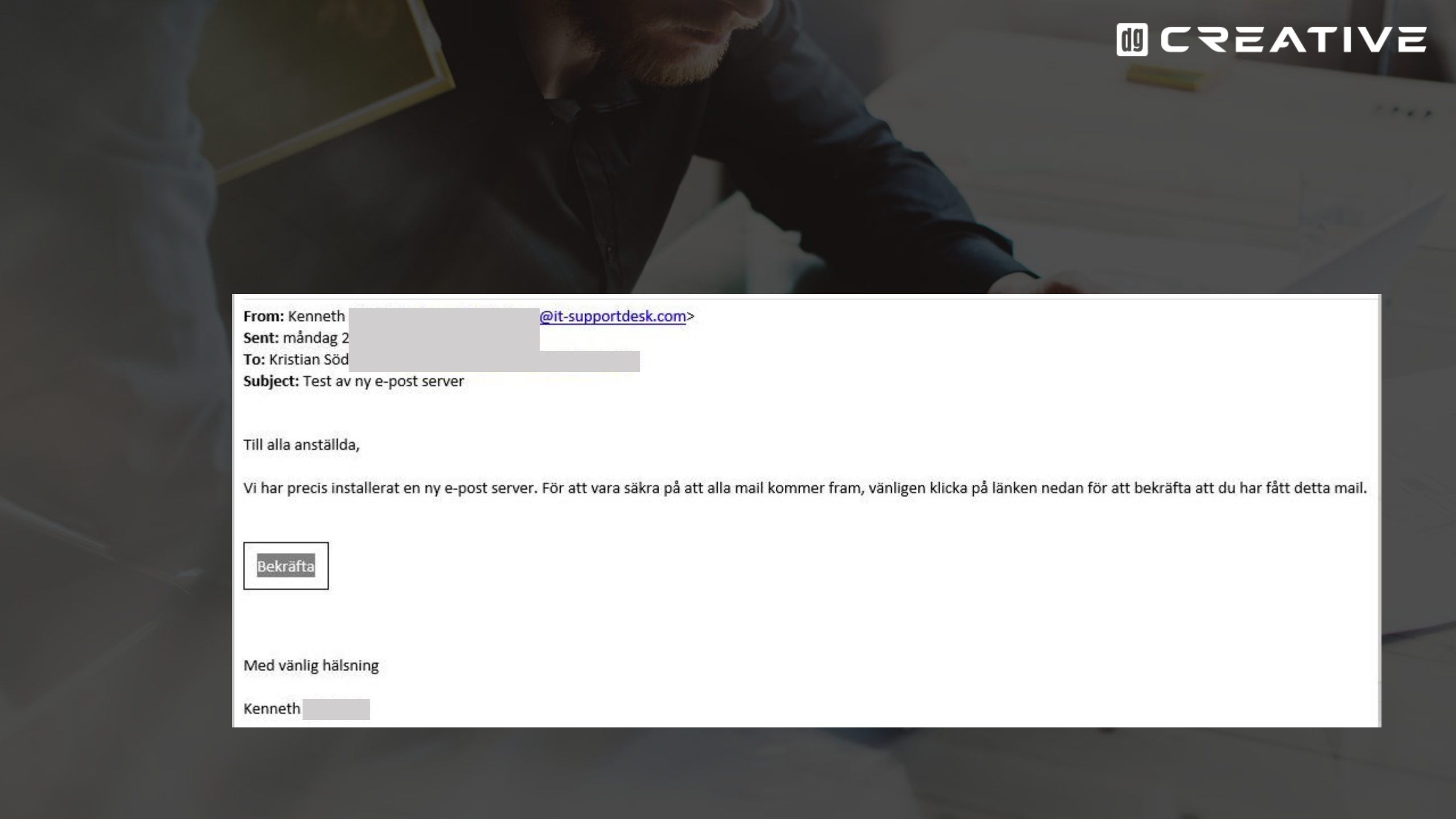
Hei Andtbacka,

Olen poissa toimistolta, mutta huomasin juuri, että unohdin kiireellisen laskun, joka on maksettava heti. Voisitko auttaa minua tässä?

Lasku löytyy verkosta - tarkista vain tämä linkki: Online_Invoice_27739.pdf

Ystävällisin terveisin
Joel Sjöblom


Failed Delivery for Joel Sjöblom
DHL <failures@dhl.trackshipping.online>(DHL via amazonses.con
To Joel Sjöblom
Reply
Reply All
Forward
ons 20-03-2019 04:06
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
DHL-Failed-Delivery.docx
13 KB
Dear Joel,
We were not able to deliver your package(s)!
For your convenience, please follow all of the instructions in the attached Failed Delivery Slip to have our drivers attempt a re-delivery or pick up your package at your local DHL office.
Attention
At your request, we can also send you the post label in order for you to print it out and take it to your nearest post office in order to pick up the package.
DHL EXPRESS - Good for Business
© DHL International GmbH. All rights reserved
Deutsche Post DHL Group



From: Kenneth @it-supportdesk.com>
Sent: måndag 2
To: Kristian Söd
Subject: Test av ny e-post server

Till alla anställda,

Vi har precis installerat en ny e-post server. För att vara säkra på att alla mail kommer fram, vänligen klicka på länken nedan för att bekräfta att du har fått detta mail.

Bekräfta

Med vänlig hälsning

Kenneth


VAD FÖRSÖKER VI SKYDDA?


MÄNNISKOR
PROCESSER
TEKNOLOGI

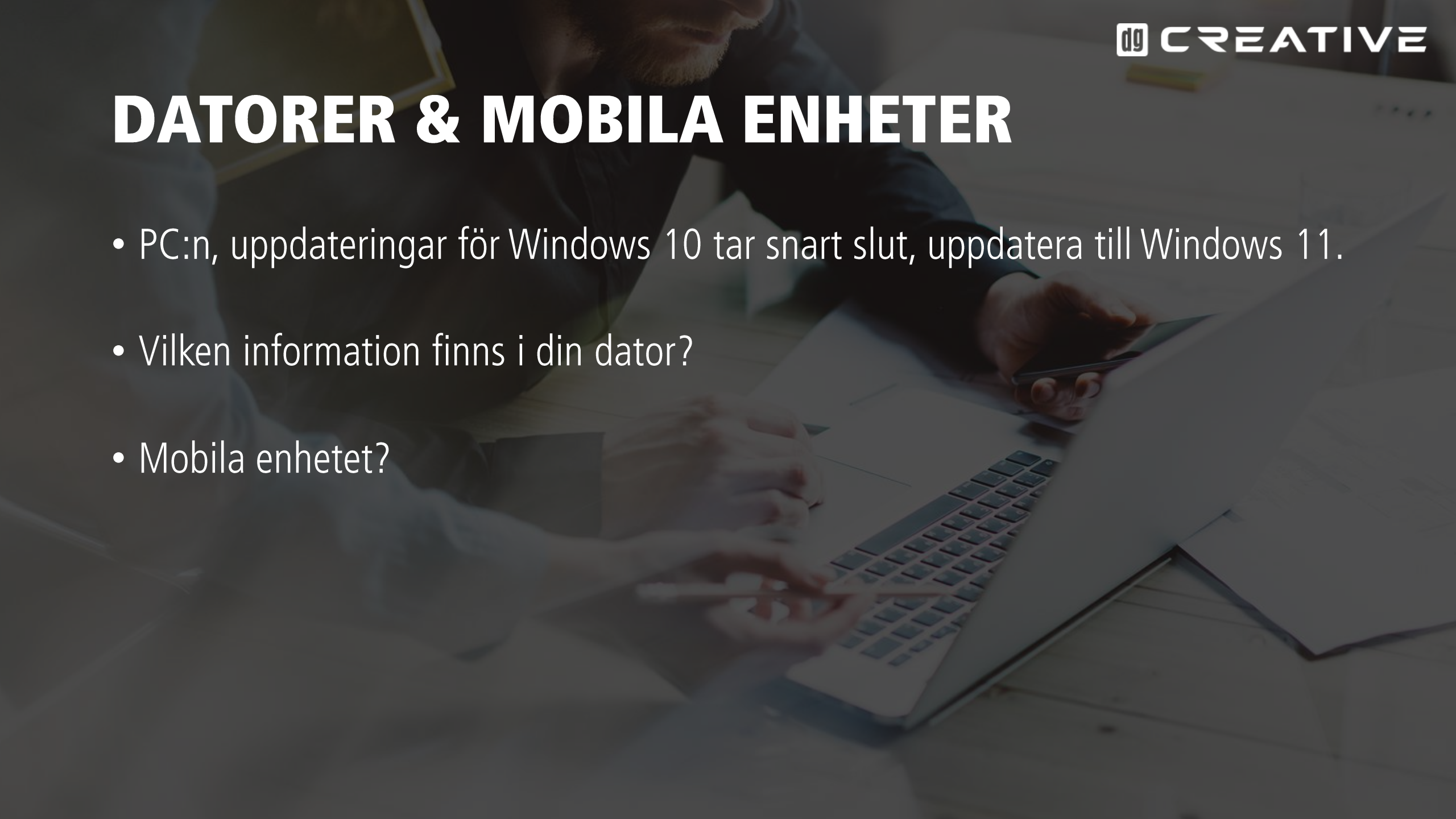

dg CREATIVE

VAD ÄR EN SÄKERHETSINCIDENT?

Exempel:

- Skadlig programvara (virus, maskar, utpressningstrojaner)
- Obehörig åtkomst (hackning, lösenordsknäckning)
- Dataintrång (obehörig ändring av eller tillgång till data)
- Extern infiltration (attacker från tredje part)
- Mänskliga fel (oavsiktligt röjande av känslig information)
- Insiderhot (anställda eller insiders som avsiktligt äventyrar säkerheten)
- Bristande säkerhetsmedvetenhet eller utbildning
- Sårbarheter i programvara eller system
- Dåligt konfigurerade eller otillräckliga säkerhetsåtgärder
- Fysiska säkerhetsöverträdelser (stöld eller förlust av enheter som innehåller känsliga uppgifter)

GRUNDLÄGGANDE SÄKERHETSPRINCIPER



DATORER & MOBILA ENHETER

- PC:n, uppdateringar för Windows 10 tar snart slut, uppdatera till Windows 11.
- Vilken information finns i din dator?
- Mobila enhetet?

Barn får ofta låna föräldrars jobbdatorer – och det är ett säkerhetsproblem

FOTO: SHUTTERSTOCK

77 procent av Sveriges föräldrar har lånat ut jobbdator eller jobbtelefon till sitt barn utan tillsyn under de senaste sex månaderna enligt en ny undersökning från Cisco där drygt 6 000 personer i EMEA-länderna deltagit. Genomsnittet för samtliga länder ligger på 56 procent.

NÄTVERK

- Skydda ditt Wi-Fi-nätverk från intrång av hackare genom att byta namnet och lösenordet på din router.
- En brandvägg skyddar ditt företags nätverkstrafik, både inkommande och utgående.
- Brandväggen kan även stoppa hackare från att attackera ditt nätverk genom att blockera vissa webbplatser.

UPPDATERINGAR

- Gamla programvaror och system är en vanlig väg in vid cyberattacker.
- Se till att alla dina system, programvaror och enheter är uppdaterade med de senaste säkerhetsuppdateringarna.
- Implementera automatiska uppdateringar där det är möjligt för att minimera risken för sårbarheter.
- Stäng av datorn!

LÖSENORD

- Desto längre lösenord, desto bättre
- Använd en lösenordshanterare
  - Bitwarden, LastPass, Keepass är exempel på gratisverktyg.
- Använd MFA – multifaktorautentisering
- En cybersäkerhetsnyckel kan vara ett bra alternativ

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

LÖSENORD

www.haveibeenpwned.com

VAR FINNS ORGANISATIONENS DATA?

MOLNLAGRINGSTJÄNSTER

- Dropbox,
- Google Drive
- OneDrive & OneDrive for Business

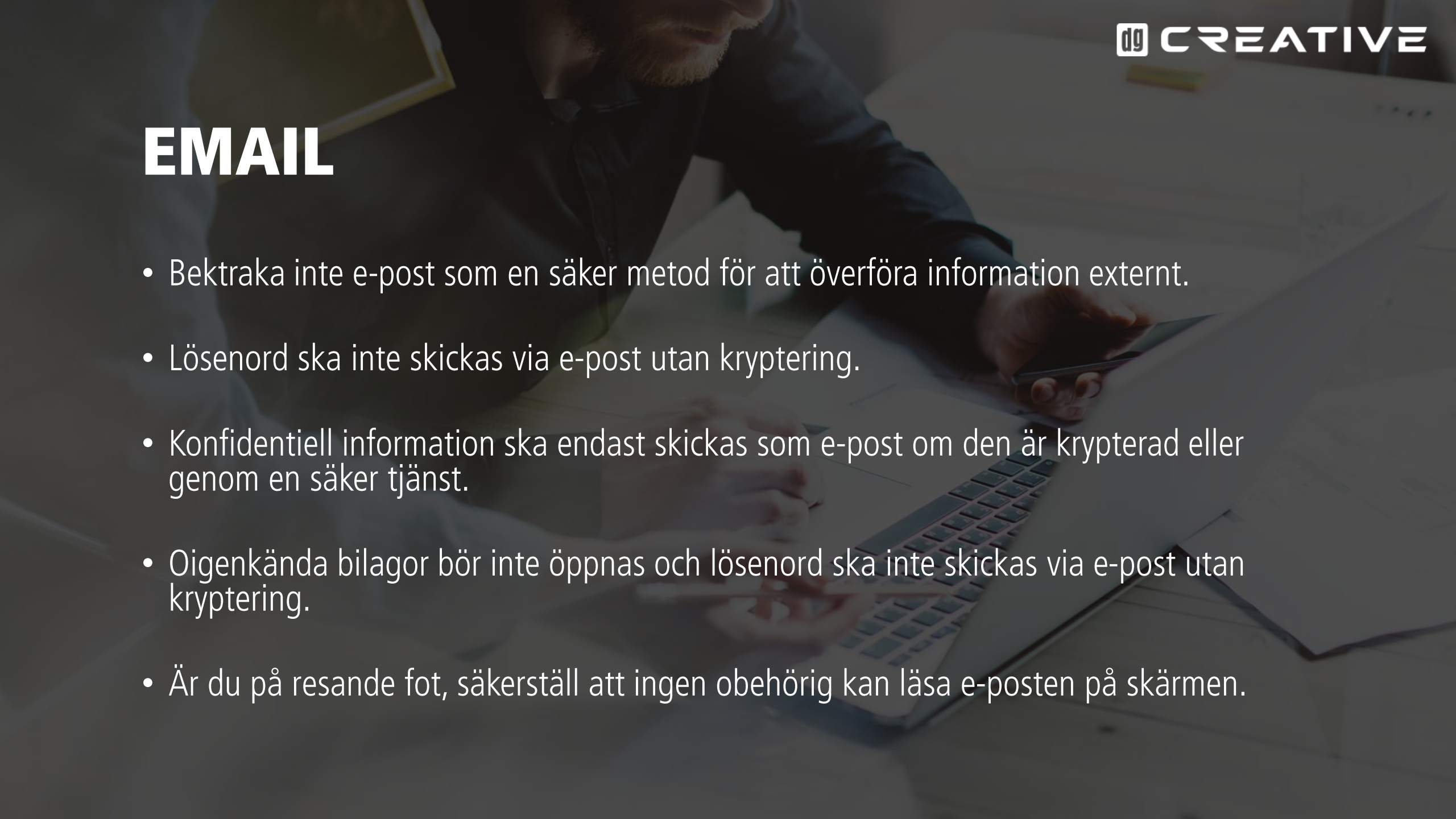
- Kom ihåg att tjänsteleverantören endast är ansvarig för att upprätthålla tjänsten, de är inte ansvariga för datan som lagras, det ansvaret är på dig.

SÄKERHETSKOPIERING AV DATA

- Kan vara avgörande för att trygga din data och företag.
- Bör göras regelbundet och helst automatiskt.
- Helst lokalt och i molnet. Har ni resurser så allra helst ska backupen vara krypterad.

EMAIL

- 2025 förväntas det sändas över 376 miljoner mail. Per dag.



EMAIL

- Bektraka inte e-post som en säker metod för att överföra information externt.
- Lösenord ska inte skickas via e-post utan kryptering.
- Konfidentiell information ska endast skickas som e-post om den är krypterad eller genom en säker tjänst.
- Oigenkända bilagor bör inte öppnas och lösenord ska inte skickas via e-post utan kryptering.
- Är du på resande fot, säkerställ att ingen obehörig kan läsa e-posten på skärmen.

ANSTÄLLDAS ROLL I SÄKERHETEN

- Utbilda anställda om datasäkerhet.
  - Hur identifierar och rapporterar man misstänkta hot.

- Ta fram policys för att hantera företagsinformation och använda privata enheter.

SUPPLY CHAIN

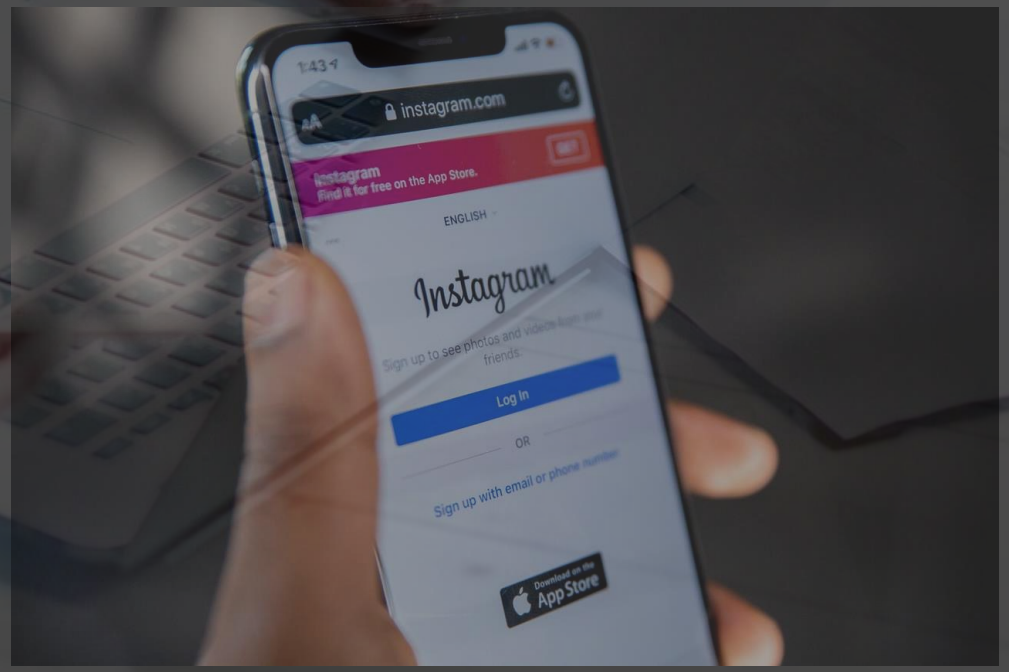
- Supply Chain attacker är en av de vanligaste metoderna för cyberattacker idag.
- Era B2B kunder kommer högst sannolikt ställa krav på er som leverantör.
- Utvärdera och säkerställ att dina leverantörer har starka säkerhetsåtgärder på plats. Inkludera säkerhetskrav i dina avtal

CLEAN DESK POLICY

Konfidentiell information ska inte lämnas obevakad på skrivbord, i mötesrum eller liknande platser. Arbetsstationer ska låsas när användaren lämnar platsen, även om det bara är för en kort stund. (Win + L)

SOCIALA MEDIER

”På offentliga platser bör diskussioner om organisationen undvikas för att förhindra informationsläckor”.
Sociala medier måste idag betraktas som en offentlig plats.



AI OCH HOT MOT SMÅFÖRETAG

- AI-drivna cyberattacker ökar
  - Automatiserade attacker – Hackare använder AI för att hitta sårbara system snabbare.
  - AI-genererad phishing – E-post och SMS som ser personliga och trovärdiga ut.
  - Deepfakes & identitetsbedrägerier – Falska röster, videor och e-post kan lura företag.

AI SOM VAPEN FÖR CYBERBROTTSLINGAR

- AI-genererade lösenordsattacker – Maskiner kan knäcka svaga lösenord på sekunder.
- Manipulerad information – AI kan sprida falska recensioner, rykten och desinformation.
- Riktade attacker – Hackare kan träna AI på offentliga data för att skräddarsy bedrägerier.

HUR SMÅFÖRETAG KAN SKYDDA SIG MOT AI-DRIVNA HOT

- Utbilda anställda om AI-bedrägerier
- Lär anställda känna igen deepfakes, AI-genererade bluffmejl & SMS.
- Genomför simulerade phishing-attacker för träning.
- Aktivera multifaktorsautentisering (MFA) på alla viktiga system.
- Uppdatera företagets säkerhetspolicy regelbundet.

DELNING AV DATA I AI-VERKTYG

- Undvik att skriva in kunddata eller interna affärshemligheter i öppna AI-chattbotar.
- Använd GDPR-kompatibla AI-verktyg.
- Ha tydliga dataskyddspolicys för hur AI används internt.

ALLMÄN DISKRETION

- Var kritisk till din omgivning när du befinner dig på offentliga platser (t.ex. tåg, flygplatser, restauranger).

- Diskutera inte frågor som rör företaget, vare sig personligen, via telefon eller andra kommunikationsmedel, om det finns risk att obehöriga kan höra eller se.

- Syftet med är att förhindra att information hamnar i fel händer.

HUR AGERA OM DU HAMNAT I EN INCIDENT?

- För dagbok och ta screen shots
- Om du misstänker att du blivit utsatt för ett dataintrång – gör en brottsanmälan
- Se *kyberturvallisuuskeskus* – de har mycket bra information, och hjälper till
- En organisation som behandlar personuppgifter som gäller dig måste meddela dig, om den drabbats av en personuppgiftsincident, som sannolikt innebär en hög risk för dina rättigheter och dina friheter.

THE DIGITAL DECADE

Skills

20 million employed **ICT specialists**, more graduates + gender balance
80% of adults can **use tech** for everyday tasks

Government

Key Public Services - 100% online
Everyone can **access health records online**
Everyone can use **eID**

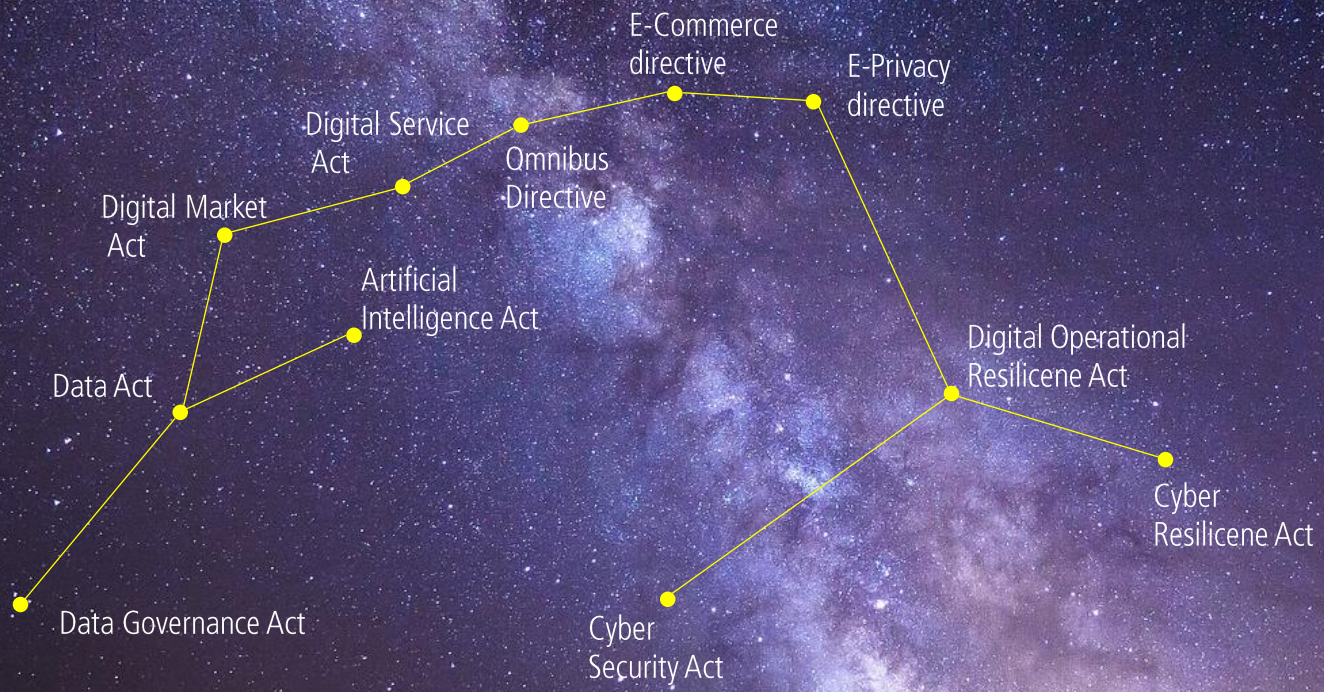
Infrastructure

Gigabit connectivity for everyone, **high-speed mobile coverage** (at least 5G) everywhere
EU produces 20% of world's **semiconductors**
10 000 **cloud edge nodes** = fast data access
EU **quantum computing** by 2025

Business

75% of companies using **Cloud, AI or Big Data**
Double the number of **unicorn startups**
90% of **SMEs taking up tech**

THE DIGITAL DECADE



TIETOSUOJAVALTUUTETUN TOIMISTO

Yritykselle huomautus asiakkaiden henkilötietojen välittämisestä työntekijöiden henkilökohtaisiin puhelimiin WhatsAppilla

8.12.2021 9.41

TIEDOTE

Tietosuojavaltuutettu on määrännyt siivousalan yrityksen muuttamaan käytäntöään, jossa asiakkaiden henkilötietoja oli välitetty työntekijöille WhatsApp-pikaviestipalvelun kautta. Käyttäessään WhatsApp-sovellusta asiakkaiden henkilötietojen käsittelyssä yritys ei ollut noudattanut velvoitteitaan huolehtia tietojen käsittelyn turvallisuudesta ja luottamuksellisuudesta tietosuoja-asetuksen mukaisesti.

Siivousyritys oli välittänyt WhatsApp-pikaviestinpalvelun kautta työntekijöiden henkilökohtaisiin puhelimiin asiakkaiden tietoja, joihin lukeutuivat esimerkiksi asiakkaiden nimet, osoitteet, puhelinnumerot, ovikoodit ja avainboksien numerot.

Tietosuojavaltuutettu toteaa, että kun sovellusta käytetään henkilökohtaisessa puhelimessa, sopimussuhde on yksityishenkilön eli työntekijän ja Facebookin välillä, eikä rekisterinpitäjällä ole keinoja valvoa, miten henkilötietoja palvelussa käytetään. Yrityksen antaman selvityksen perusteella se ei myöskään ollut kertonut asiakkailleen WhatsAppin käytöstä henkilötietojen käsittelyssä.

Yrityksen käytäntö ei vastannut tietosuoja-asetuksessa määriteltyä sisäänrakennetun ja oletusarvoisen tietosuojan vaatimusta, jonka mukaan rekisterinpitäjän on otettava tietosuoja huomioon henkilötietojen käsittelyssä alusta alkaen. Tietosuojavaltuutettu antoi yritykselle huomautuksen tietosuoja-asetuksen vastaisesta henkilötietojen käsittelystä ja määräsi sen muuttamaan toimintatapansa tietosuojasäännösten mukaiseksi.

WhatsAppin käyttö johtaa todennäköisesti henkilötietojen siirtämiseen EU:n ulkopuolelle

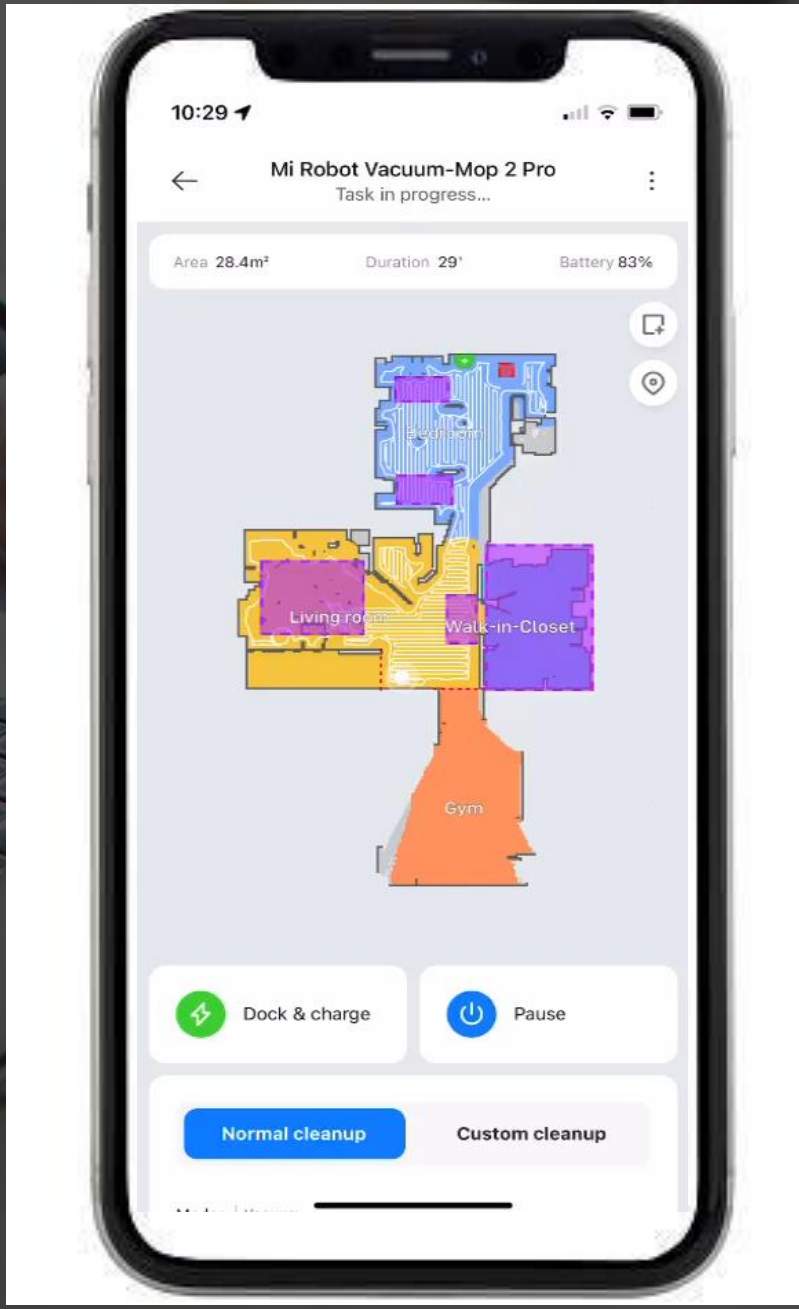
Tietosuojavaltuutettu kiinnittää päätöksessään erityistä huomiota siihen, että WhatsApp-sovelluksen käyttö on todennäköisesti johtanut asiakkaiden henkilötietojen siirtoon EU:n alueelta kolmansiin maihin, kuten Yhdysvaltoihin.

Kesällä 2020 EU-tuomioistuin totesi niin sanotussa Schrems II -ratkaisussaan (C-311/18) EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn pätemättömäksi, koska tiedonsiirroissa EU:n ja Yhdysvaltojen välillä ei ollut turvattu riittävää tietosuojan tasoa. Ratkaisun mukaan rekisterinpitäjän on keskeytettävä henkilötietojen siirrot kolmanteen maahan, jos se ei voi toteuttaa riittäviä lisätoimenpiteitä henkilötietojen suojan varmistamiseksi.

Tiedonsiirtojen osalta tietosuojavaltuutettu ei käyttänyt korjaavia toimivaltuuksiaan, sillä asian selvitystyö tehtiin ennen kuin EU:n tiedonsiirtoja koskevia ohjeistuksia ja siirtomekanismeja päivitettiin Schrems II -ratkaisun myötä.

SMART TECHNOLOGY

- The Hyppönen law – *if it´s smart – it´s vulnerable*



SAMMANFATTNING

- Vaksam på vad du klickar. Nätfiske är fortsatt den vanligaste vägen in.
  - sms, email, samtal
- Uppdatera dina enheter
  - Datorer, mobila enheter, smarta enheter
- Använd MFA överallt där det går
- Använd anti-virus på dina enheter
- Säkerhetskopiera och säkerställ att den fungerar
- Utnyttja AI-tjänster, men dela aldrig med dig av känslig information

dg CREATIVE

TACK!