



Business Email Compromise

Context is key

Donderdag 18 september 2025



Thomas Schrader

linkedin.com/in/thomassebastiaanschrader/



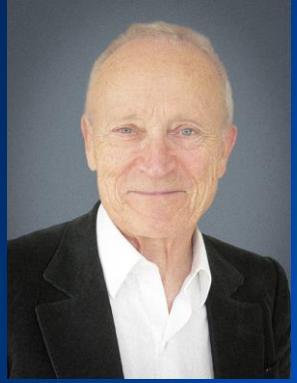
Bram Zegwaart

linkedin.com/in/zmarb

Microsoft Defender for Office 365





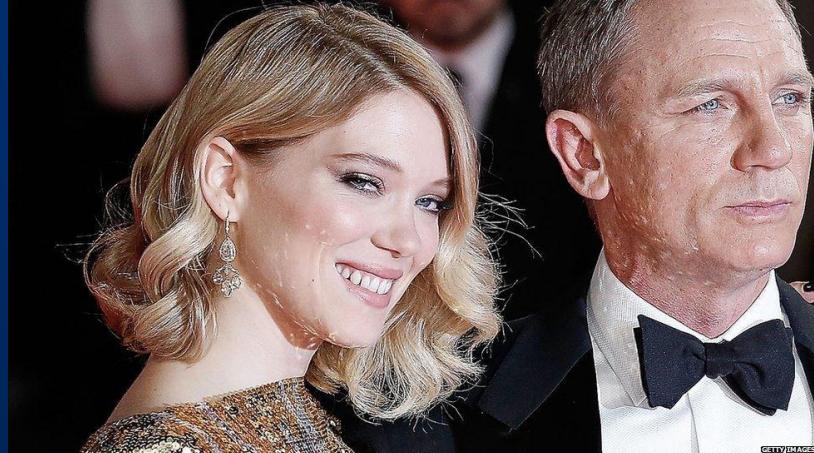


Jérôme Seydoux



Sophie Seydoux

Family-owned group



Cinémas

France

Africa

Belgium

Switzerland

The
Netherlands

Pathé
International



Films

Switzerland

United
Kingdom

Hoe de top van Pathé voor €19 mln om de tuin werd geleid

Job Woudt 9 nov '18

Een ceo-fraude kostte twee topfunctionarissen van bioscoopexploitant Pathé dit voorjaar de kop. In een recent vonnis van de rechtbank Amsterdam wordt uit de doeken gedaan hoe de oplichters te werk gingen.



Op donderdag 8 maart 2018 komt er een e-mail binnen bij Dertje Meijer, topvrouw van Pathé Nederland. Afzender: de ceo van haar Franse moederbedrijf. Of KPMG al contact met haar had opgenomen die ochtend? Het bericht is afkomstig van een smartphone.

Ze speelt de vraag door naar de financieel directeur, Edwin Slutter. Het verzoek zegt ook hem niets. Terugmailen dan maar weer: hoezo, waarom, wat is er?

Dan komt de reden: 'We zijn op dit moment bezig met een financiële transactie, die betrekking heeft op de overname van een buitenlandse onderneming in Dubai.'



Pathé City in Amsterdam. Foto: Harold

Key stakeholders



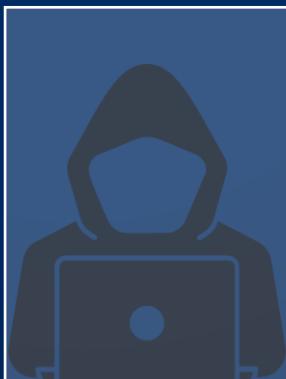
Dertje Meijer
CEO Pathé NL



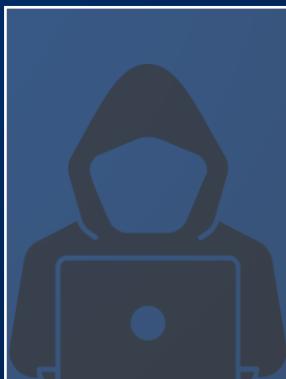
Edwin Slutter
CFO Pathé NL



Finance Department
Pathé International



Eduardo Malone
CEO Pathé Int.



Accountant
KPMG Canada



woensdag 8 maart 2018 | 1^e mail ontvangen

Please contact Mr ... from KPMG immediately via email ... to obtain the opposing party's banking information in order to proceed with the transfer of the first installment in the amount of EUR 826,521 (first 10%).

donderdag 9 maart 2018 | Bevestiging en factuur eerste betaling

Thank you to do the necessary while respecting the strictest confidentiality. Find attached the invoice (signed) for this payment. Invoice from Towering Stars General Trading LLC

maandag 13 maart 2018 | 2^e betaling

Second tranche of EUR 2.479.563,00 (signed invoice). Request of EUR 5.0M from cash pool of Pathé International.

donderdag 16 maart 2018 | 3^e betaling

Third tranche of 30% is paid.

maandag 20 maart 2018 | Gelden ontvangen vanuit Frankrijk

Pathé International released the requested fund from cash pool and Pathé NL confirmed the fourth tranche.



donderdag 22 maart 2018 | 5^e betaling

Fifth tranche of EUR 5.826.770,00 based on signed invoice.

maandag 26 maart 2018 | wederom cash-pool aanvraag richting Frankrijk

Pathé NL received an additional payment request, after which Pathé NL submitted a second cash pool request.

dinsdag 27 maart 2018 | Laatste betaling

Final tranche of EUR 5.152.354,00 based on signed invoice again.

woensdag 28 maart 2018 | Vragen vanuit Pathé International

Bad actors confirmed payment, and they would ensure that the withdrawn amounts, totaling **€19,244,304,00**, would be refunded the following day.

Questions came from France about the amounts requested from the cash pool. During a telephone consultation that same day, it became clear that Pathé had become the victim of a so-called **CEO fraud**.



Vrijdag 30 maart 2018 | Ontslag CEO en CFO
Pathé's directeuren Dertje Meijer en Edwin Slutter per direct weg.



Dertje Meijer
CEO Pathé NL



Edwin Slutter
CFO Pathé NL



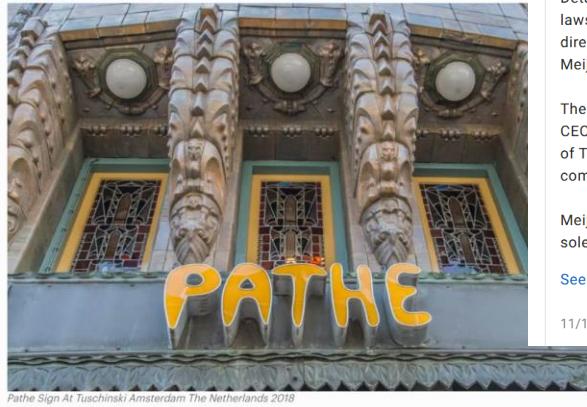
NOS Nieuws • Zaterdag 10 november 2018, 10:31

Pathé voor 19 miljoen euro opgelicht door nepmails 'hoofdkantoor'

Bioscoopketen Pathé is slachtoffer geworden van een overname in het buitenland.

19 miljoen euro is buitgemaakt. Criminelen hebben het Franse hoofdkantoor en stuurden e-mails met de verzoek om geld over te maken, melden vaders van de rechter deze week over de veroordeling.

Zo wordt aan de tweekoppige directie gevraagd om een overname in het buitenland te bekijken. Niemand op de hoogte te stellen van de transactie. In de mail wordt ook verzoek om geld over te maken. De Nederlandse directie kan toch mee.



Pathe Sign At Tuschinski Amsterdam The Netherlands 2018
GETTY

De Telegraaf NIEUWS SPORT ENTERTAINMENT FINANCIËL VROUW LIFESTYLE

Overzicht Nieuws Koersen Geld Ondernemen Carrière Stan Huygens Journaal

VOORPAGINA / FINANCIËL

Lees voor ▶

Pathé-directie kinderlijk simpel opgelicht

Door PIETER VAN ERVEN DORENS 10 nov. 2018 IN FINANCIËL

AMSTERDAM (DFT) - Hoe konden Pathé-topvrouw Dertje Meijer en financieel directeur Edwin Slutter zo dom, of in ieder geval naïef zijn, om €19 miljoen over te maken aan internetfraudeurs? Die vraag bekrijgt je bij het lezen van het juridisch verslag van deze fraude.

IMDb Menu All Search IMDb

Cinema Chain Sees Bad Movie Script Play Out As It Loses Millions In Email Scam

By Martijn Grootenhuis, Former Contributor. I write about all aspects of cybersecurity.

Nov 12, 2018, 03:12pm EST

Share Save

This article is more than 6 years old.

Pathé Loses More Than \$21 Million in Internet Scam

France's leading independent film group, **Pathé**, recently lost €19.2 million (\$22 million) in an internet scam that targeted the mini-major's Dutch office.

Details of the scam were contained in an Oct. 31 ruling by the District Court of Amsterdam on a lawsuit against Pathé for unfair dismissal filed by Edwin Slutter, Pathé Netherlands' former financial director. Slutter was fired, along with Pathé Netherlands' former CEO and managing director, Dertje Meijer, in April after the scam was discovered.

The fraud kicked off in March with several emails apparently sent from the personal account of Pathé CEO **Marc Lacaen** to **Meijer**, asking her to wire up to €19.2 million in four tranches to the bank account of Towering Stars General Trading LLC in Dubai. The funds were supposedly to be used to acquire a company in Dubai.

Meijer was asked to respect the "strictest confidentiality" about the transaction and exchange emails solely with Lacaen...

See full article at [Variety Film + TV](#)

11/13/2018 • by Elsa Keslassy • [Variety Film + TV](#)

IBM AI Hybrid Cloud Products Consulting Support

Think Think 2025 Artificial intelligence Cloud Security Videos Reports

example:

- In 2015, [Ubiquity Networks](#) lost nearly USD 47 million in just 17 days when whale phishing attackers impersonating the company's CEO and Chief Counsel sent emails convincing the Chief Accounting Officer to make a series of wire transfers to finance a secret acquisition.
- In 2018, [Pathé Film Group](#) lost EUR 19.2 million (USD 21 million) when scammers pretending to be the CEO at Pathé's headquarters in France emailed the CEO of Pathé's Netherlands office, requesting wire transfers to fund an acquisition.

VARIETY

Pathé Loses More Than \$21 Million in Internet Scam

Elsa Keslassy

Updated Tue, November 13, 2018 at 6:01 PM GMT+1



France's leading independent film group, **Pathé**, recently lost €19.2 million (\$22 million) in an internet scam that targeted the mini-major's Dutch office.

Details of the scam were contained in an Oct. 31 ruling by the District Court of Amsterdam on a lawsuit against **Pathé** for unfair dismissal filed by Edwin Slutter, Pathé Netherlands' former financial director. Slutter was fired, along with Pathé Netherlands' former CEO and managing director, Dertje Meijer, in April after the scam was discovered.

Cyber Security + Add to myFT

'London Blue' hacker group targets chief financial officers

List of 50,000 targets found by cyber security firm Agari

'London Blue' hacker group targets chief financial officers

List of 50,000 targets found by cyber security firm Agari



Hannah Kuchler in San Francisco

Published DEC 4 2018



A hacker group has compiled a list of 35,000 chief financial officers, including some at the world's biggest banks and mortgage companies, so as to target them with bogus requests to transfer money.

The "London Blue" hackers are the latest group to focus on "business email compromise" campaigns, according to the cyber threat detection company Agari, which found a list of 50,000 targets, most of whom worked in accounting departments.

own chief financial officer with a spoof email that purported to be from the chief executive — a practice known as "whaling" because a hacker disguises themselves as one of the biggest fish at the company. Agari engaged with the attackers to find out more about which bank accounts they were using to take transactions.

list of 35,000 chief financial officers, including banks and mortgage companies, so as to target them with bogus requests to transfer money.

the latest group to focus on "business email compromise" campaigns, according to the cyber threat detection company Agari, which found a list of 50,000 targets, most of whom worked in accounting departments.

This type of scam — where a chief financial officer is tricked into sending money to an unknown account — is on the rise and has cost banks and companies \$12bn since 2013, with the number of victims increasing every year.

According to US and UK law enforcement agencies. If the hackers are found to be based in the UK and US, it could lead to legal action in those countries and other territories.

Mr Hassold, director of threat research at Agari, said it had seen some success in some cases, including a bank's loss prevention unit that a transaction for \$100,000 was flagged as suspicious.

Mr Hassold said, as the attack depends on social engineering rather than sophisticated technology. "The reason it has been proven to work."

In one case, a hacker tried to trick the cyber security company's own chief financial officer with a spoof email that purported to be from the chief executive — a practice known as "whaling" because a hacker disguises themselves as one of the biggest fish at the company. Agari engaged with the attackers to find out more about which bank accounts they were using to take transactions.

In de media

NOS Nieuws • Zaterdag 19 oktober, 16:53

Hacker knoeit met facturen: Limburgs Schuttersfeest voor 78.000 euro gedupeerd

De organisatie van het Oud-Limburgs Schuttersfeest (OLS) is voor tienduizenden euro's opgelicht door phishing. De fraudeur is binnengedrongen in de systemen van de organisatie en kon zo 78.000 euro wegsluizen.

De oplichter gebruikte daarvoor facturen van leveranciers. Door bankrekeningnummers op die facturen aan te passen ging het geld niet naar de

Nep-aanmaning
'Menselijke fout': gemeente Helmond voor bijna een ton opgelicht

Door RTL Nieuws · 25 november 2024 · Aangepost: 25 november 2024



De gemeente Helmond heeft in september een bedrag van 93.000 euro overgemaakt aan onbekenden. De gemeente traptte in een nep-aanmaning die via de mail binnenkwam.

Net binnen Algemeen Economie Sport Media en Cultuur Achterklap Shop Meer



Hack op politie vermoedelijk uitgevoerd via gestolen cookies

Door Tweakers

security.nl presented by Certified Secure

Nieuws Achtergrond Community

Antivirusbedrijf meldt ransomware-aanvallen via Microsoft Teams "helpdesk"

dinsdag 21 januari 2025, 14:50 door Redactie, 0 reacties



Meerdere organisaties zijn de afgelopen weken het doelwit geworden van ransomware-aanvallen die begonnen via Microsoft Teams, zo meldt antivirusbedrijf **Sophos**. De virusbestrijder zag de afgelopen drie maanden vijftien incidenten, waarvan de helft in de afgelopen twee weken. De aanvallers gebruiken hun eigen Office 365-omgeving om via Microsoft Teams contact met het doelwit op te nemen. Microsoft Teams staat standaard toe dat gebruikers een extern domein chats of meetings met interne gebruikers kunnen starten, stelt Mark Parsons van Sophos.

De aanvallers sturen de organisaties eerst een grote hoeveelheid spamberichten. Vervolgens nemen de aanvallers vanaf hun eigen Office 365-omgeving contact op met het doelwit. Daarbij doen de aanvallers zich voor als de "helpdesk". Tijdens het gesprek, dat via Microsoft Teams plaatsvindt, geven de aanvallers het doelwit instructies om een remote screen control session via Teams toe te staan. Zodra het doelwit dit doet kan de aanvaller malware op het systeem van deze gebruiker

Context binnen Business Email Compromise

Gegevensdiefstal

Kwaadwillende richten zich eerst op specifieke actoren om persoonsgegevens te verzamelen. Het is dan eenvoudiger om geloofwaardige BEC-scams uit te voeren.

CEO-fraude

Scammers spoofen of hacken het e-mailaccount van een CEO. De kwaadwillende stuurt een verzoek richting een potentieel slachtoffer.

Accountcompromittering

Gebruiken phishing of malware om toegang te krijgen tot het e-mailaccount van een financieel medewerker.

Nepfacturen

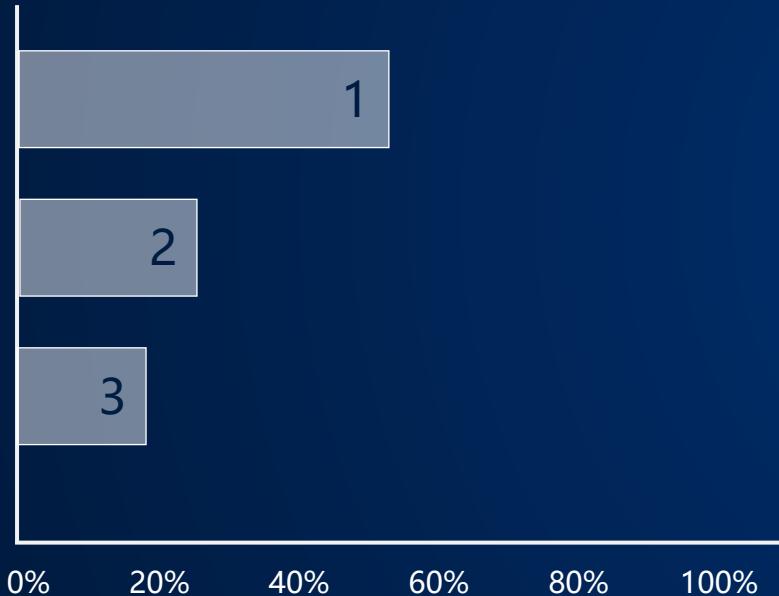
De scammer doet zich voor als een legitieme leverancier waarmee je bedrijf werkt, en e-mailt een neprekening – die vaak heel erg op een echte lijkt.

Imitatie, zich verdoen als (impersonation)

Onbevoegde krijgen toegang tot een emailaccount van een organisatie. Kwaadwillende acteren vervolgens uit naam van de organisatie van het verkregen emailccount richting potentiële slachtoffers.

Geavanceerde business email compromise technieken

Steeds meer malicious sign-in pagina's bevatten AiTM mogelijkheden welke sommige MFA methodes kunnen omzeilen



Bron: Microsoft Digital Defense Report 2024

1. Phishing URL/link (56%)
2. QR code phishing (25%)
3. Phishing attachments (19%)



Cybersecuritybeeld Nederland 2024

Generatieve AI van invloed op digitale veiligheid

Het gebruik en de mogelijkheden van generatieve AI zijn zich nog volop aan het ontwikkelen en de impact op de samenleving kent nog vele onduidelijkheden. Er zijn in ieder geval vier relevante invalshoeken. Ontwikkelingen binnen en inzet van generatieve AI vallen hier tot nu toe onder:

1. De algoritmen en de data waarmee de algoritmen worden gevoed kunnen doelbewust worden gemanipuleerd. Dat kan bijvoorbeeld door middel van cyberaanvallen.
2. Gebruikers kunnen (onbedoeld en onbewust) toegang geven tot zoekvragen en/of gevoelige informatie door de vragen die ze stellen, de informatie die ze invoeren of de informatie waarmee ze de applicaties voeden.

3. Generatieve AI kan worden gebruikt voor cyberaanvallen. Zo kunnen met behulp van AI meer op een ontvanger toegesneeden phishing-mails worden gemaakt. Verder kunnen kwaadwillenden generatieve AI gebruiken om snel en automatisch interessante doelwitten te detecteren en informatie daarover te verzamelen. Ook kan laagdrempeliger malware worden ontwikkeld.
4. Generatieve AI kan worden ingezet ter verdediging tegen cyberaanvallen door bijvoorbeeld onregelmatigheden te detecteren in data.

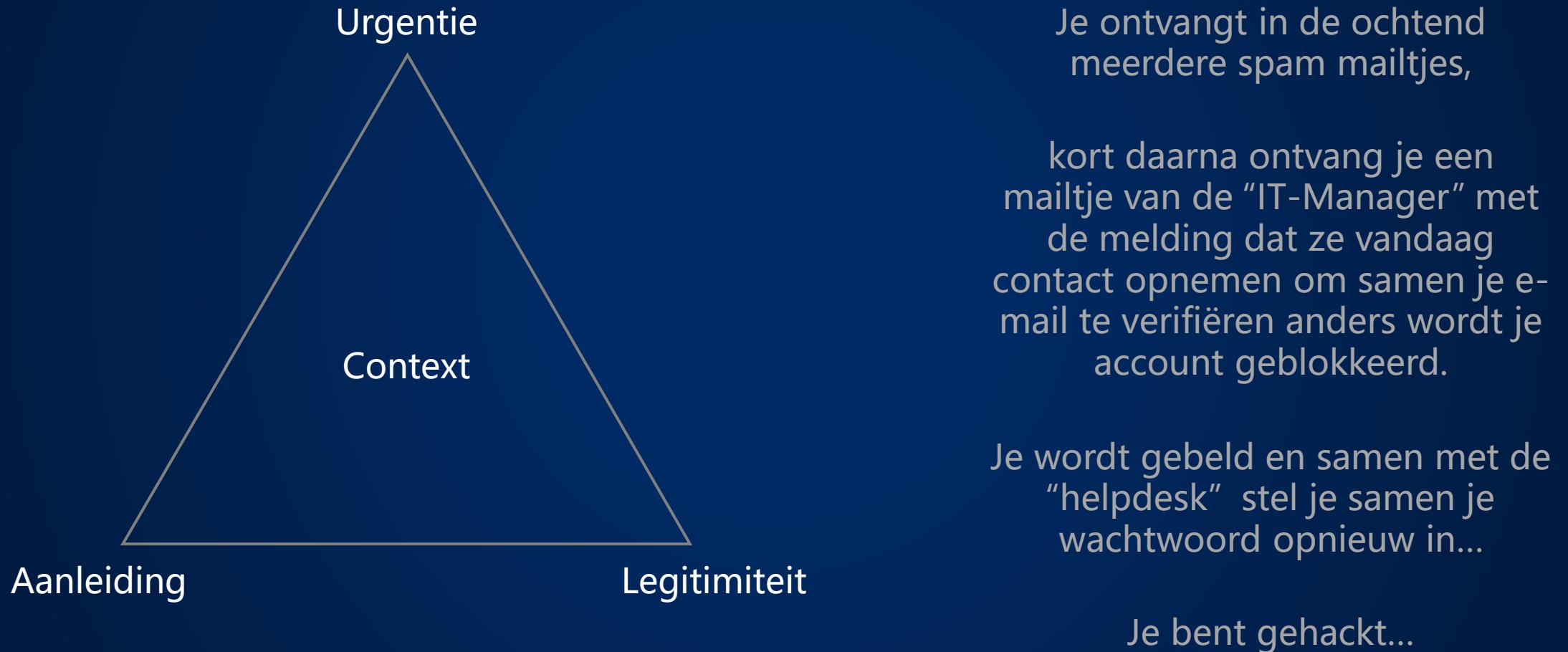
Cybersecuritybeeld Nederland 2024



Kwaadwillenden kiezen vaak weg van minste weerstand

Kwaadwillenden gaan nog altijd veelal voor aanvalsroutes die relatief eenvoudig en snel toegang bieden. Actoren maken nog altijd veel gebruik van (spear)phishing. Daarbij worden e-mails verstuurd die betrouwbaar en relevant lijken, maar deze bevatten

Social engineering



Bedrijfsinformatie

Rubicon Consulting & Technology's LinkedIn profile features a banner with the text "BUILDING BEYOND TECHNOLOGY". The profile includes a summary about being a partner for digital transformation, cloud adoption, and AI implementation, located in Leusden, Utrecht, with 7,000 members. It shows buttons for following, messaging, and more.

Rubicon Cloud Advisor

Partner voor digitale transformatie, cloud adoptie en AI implementatie
IT-services en consultancy · Leusden, Utrecht · 7.000 volgers · 201-500 medewerkers

+ Volgen Bericht sturen ...

[Home](#) [Info](#) [Bijdragen](#) [Vacatures](#) [Wat we doen](#) [Personen](#)

Overzicht

Rubicon is Nederlands beste Microsoft, cloud-native, partner om voor én mee te werken. Onze co-create hub op landgoed Leusderend, is dé broedplaats voor ervaren Microsoft cloud experts. Daar zijn we best trots op. Rubicon's cloud specialisten behalen succes door een Agile aanpak, open mindset en de meest innovatieve Microsoft cloud & AI technologie toe te passen in de oplossingen voor onze klanten.

[Alle details weergeven →](#)

Overview

Rubicon is Nederlands beste Microsoft, cloud-native, partner om voor én mee te werken. Onze co-create hub op landgoed Leusderend, is dé broedplaats voor ervaren Microsoft cloud experts. Daar zijn we best trots op. Rubicon's cloud specialisten behalen succes door een Agile aanpak, open mindset en de meest innovatieve Microsoft cloud & AI technologie toe te passen in de oplossingen voor onze klanten.

Met onze diensten bedienen we de financiële sector, de Nederlandse overheid en de grootzakelijke markt. Onze focus ligt altijd op de juiste oplossing voor iedere organisatie. Dit realiseren we met vakkundig maatwerk óf met de inzet van slimme Rubicon solutions. Altijd transparant en Agile. Het doel en jouw bedrijfsucces zijn voor ons leidend.

Als gespecialiseerde ICT dienstverlener mag je van ons hoogwaardig advies op maat verwachten met de beste oplossingen. Onze deskundigheid rijkert van consultancy tot implementatie en beheer. Als Microsoft Specialized Partner, zijn we dé expert in ons vakgebied.

Website

<http://www.rubicon.nl>

Phone

[088 240 73 65](tel:0882407365)

Verified page

September 12, 2023

Industry

IT Services and IT Consulting

Company size

201-500 employees

471 associated members

Headquarters

Leusden, Utrecht

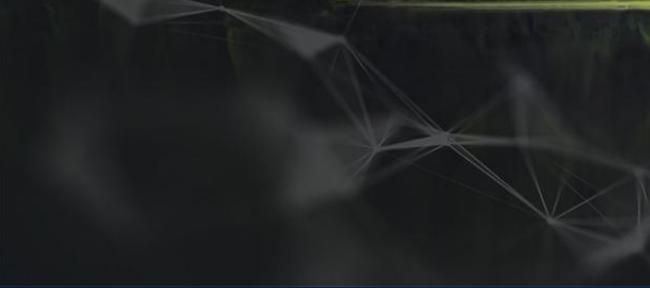
Founded

1998

Profiling op basis van OSINT



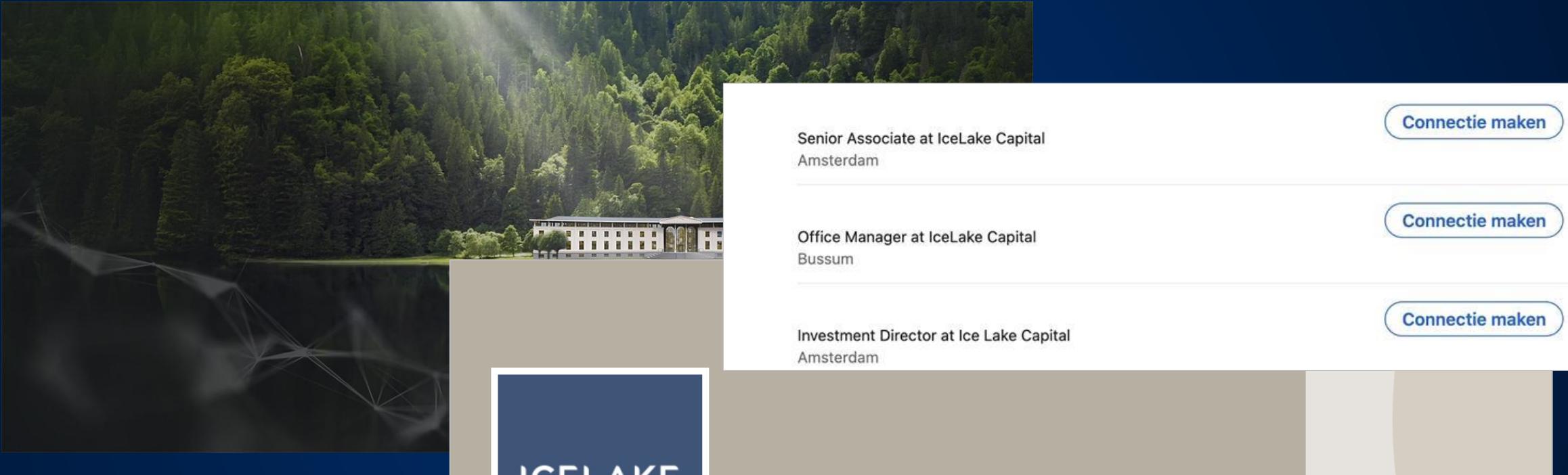
Profiling op basis van OSINT



IceLake

Durfkapitaal en privévermogen · Amsterdam, North Holland · 3.000 volgers · 2-10 medewerkers

Profiling op basis van OSINT



ICELAKE

IceLake
Durfkapitaal en privévermogen · Amsterdam, North Holland · 3.000 volgers · 2-10 medewerkers

Senior Associate at IceLake Capital
Amsterdam

[Connectie maken](#)

Office Manager at IceLake Capital
Bussum

[Connectie maken](#)

Investment Director at Ice Lake Capital
Amsterdam

[Connectie maken](#)

Zoeken naar legitimiteit

Autoriteit
Consument & Markt



[ACM](#) > [Publicaties](#)

**Ice Lake
zeggense
Consulting
(concent**

Investeerder Icelake strijkt neer in België met overname Studibo



Het project ZIN in de Noordwijk is een van de werven waaraan Studibo - via de akoestiekspécialist Bureau De Fonseca - meewerkte. ©Kristof Vadino

team

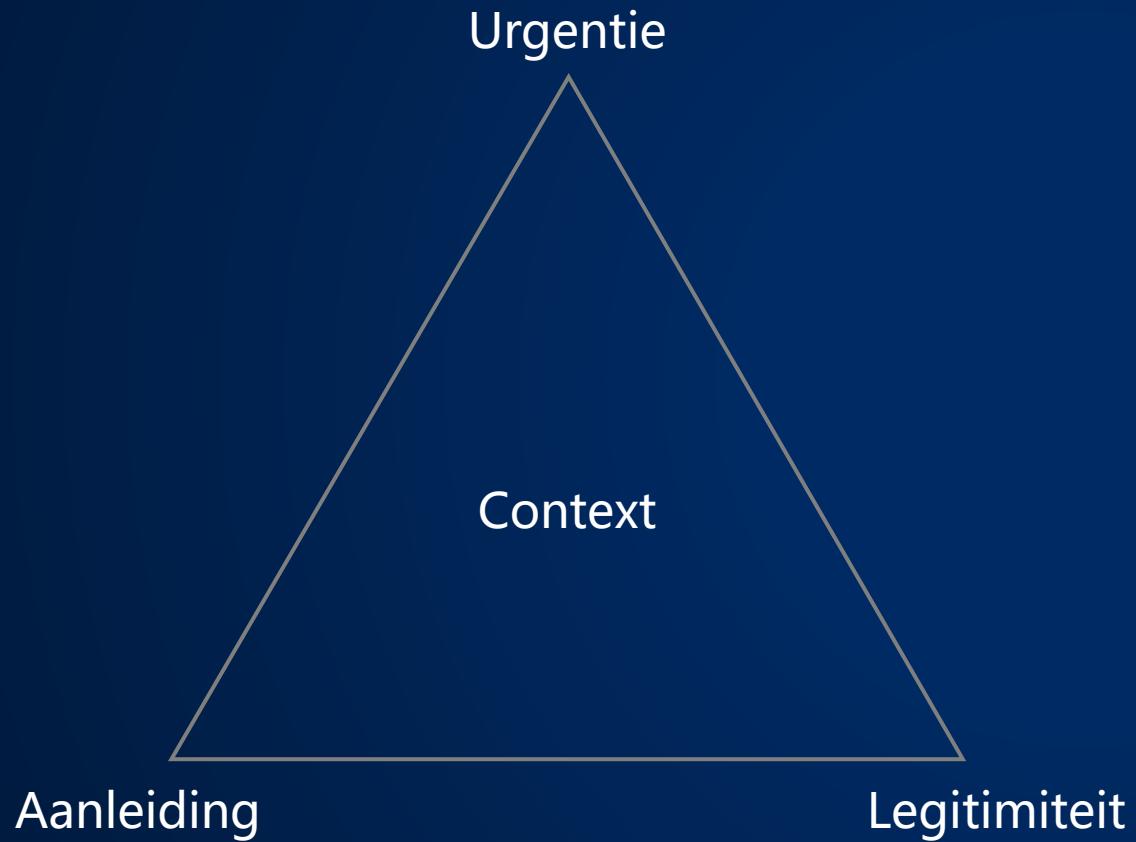
Rotterdam 3

AI 3

Zuid/Oost 2



Social engineering



De CEO/CFO van Rubicon ontvangt een mail vanuit "IceLake" dat ze bezig zijn met een acquisitie van een AI partij in België ter uitbreiding van Navara Consultancy.

"IceLake" geeft aan dat "Navara" contact zal opnemen met een hulpvraag voor een gedegen technische due diligence op het IP van de organisatie voor het einde van de maand.

"Navara" deelt haar bevindingen via een online Excel waarvoor ingelogd moet worden met je bedrijfsaccount.

De CxO is gehackt...

Impersonation vs spoofing

Impersonation

een vorm van digitale oplichting waarbij kwaadwillende een valse identiteit aannemen om te misleiden, te bedriegen en toegang te krijgen tot geld of persoonlijke gegevens.

Spoofing

Een technische handeling om een bron te laten lijken op een andere vertrouwde bron door informatie technisch te vervalsen zoals een emailadres of telefoonnummers.

Aanvalsmethodes CEO-fraude

Methode Email spoofing



Methode via een compromised account

Impersonation via gecompromitteerd account vanuit organisatie of leverancier.

Impersonation of the domain

contoso.com vs cónotoso.com

User impersonation

Marnix Huizinga <mhuizinga@gmail.com>

HYMOGLYPH ATTACK

PHISHING

AiTM ATTACK

Layered email security...



Safe Links

URL scanning



Safe Attachments

Uses a sandbox to check attachments



Anti-phishing

Impersonation protection

Mailbox intelligence

Microsoft Defender for Office 365 (MDO)



Anti-spam

reduce junk



Anti-malware

viruses, spyware and ransomware



Anti-phishing

spoof intelligence

Exchange Online Protection (EOP)

SPF

DKIM

DMARC

DANE

DNSSEC

Anti-spam features



Anti-spam

Inbound policy

- Bulk Compliant Level (BCL) | Default setting: 7, recommended setting: 6
- Activeer spam safety tips
- Activeer zero-hour auto purge (ZAP) voor phishing en spam
- Quarantine policy | AdminOnlyAccessPolicy

Connection filter policy

- IPAllowList is leeg

Outbound policy

- Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups

Anti-malware features



Anti-malware

-
- Activeer zero-hour auto purge (ZAP) voor malware | Quarantine message
 - Activeer common attachments filter | Reject the message with a non-delivery report (NDR)
 - Quarantine policy | AdminOnlyAccessPolicy

Anti-phishing features



Anti-phishing

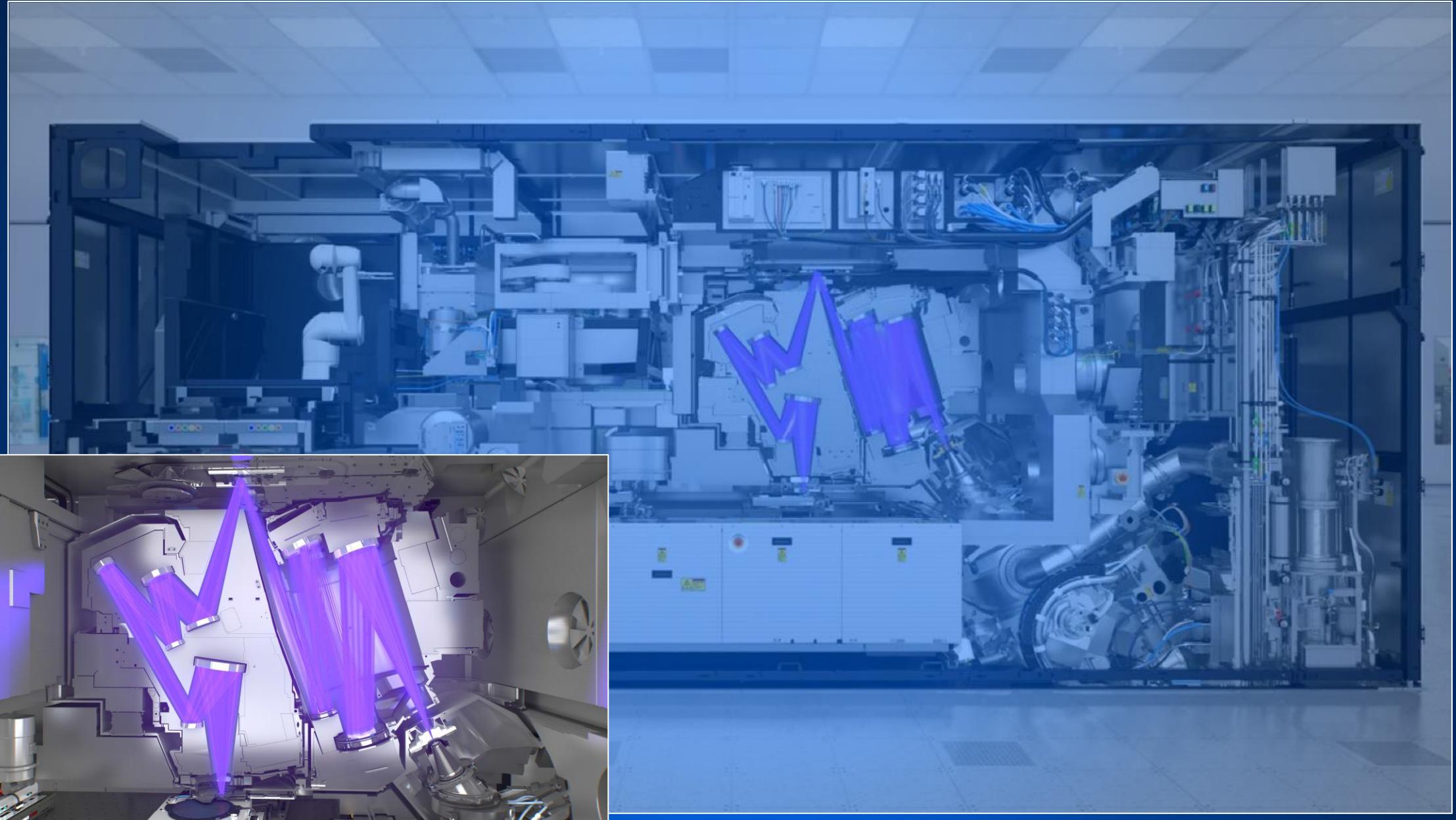
-
- Anti-phishing is onderdeel van elke cloud mailbox (Spoof intelligence)
 - Impersonation protection is onderdeel van Defender for Office 365 Plan 2
 - Beveiliging van de ontvanger, het domein en de afzender
 - Defineer afzenders en domeinen om false positive te beperken
 - Belangrijk om te definiëren:
 - Wie zijn je belangrijkste stakeholders? C-level, Management, HR & IT. (maximaal 350 personen)
 - Hoe ziet de keten eruit?
Partners & leveranciers en welke domeinen horen daar bij?

Anti-phishing features



Anti-phishing

- Hanteer waarde "3 - More Aggressive" als Phishing email threshold.
- Activeer spoof intelligence
- Activeer mailbox intelligence
- Activeer intelligence for impersonation protection
- Quarantine messages
- Activeer safety tips



Organisatorische maatregelen

- Communiceer over het beveiligingsbeleid
- Meldpunt voor security vragen
- Jaarlijkse security campagne
- Cybersecurity is een verantwoordelijkheid van iedere medewerker
- Verifieer bij onzekerheid!



Bron: Board toolkit from National Cyber Security Centre (NCSC UK)

Organisatorische maatregelen

- Communiceer over het beveiligingsbeleid
- Meldpunt voor security vragen
- Jaarlijkse security campagne
- Cybersecurity is een verantwoordelijkheid van iedere medewerker
- Verifieer bij onzekerheid!

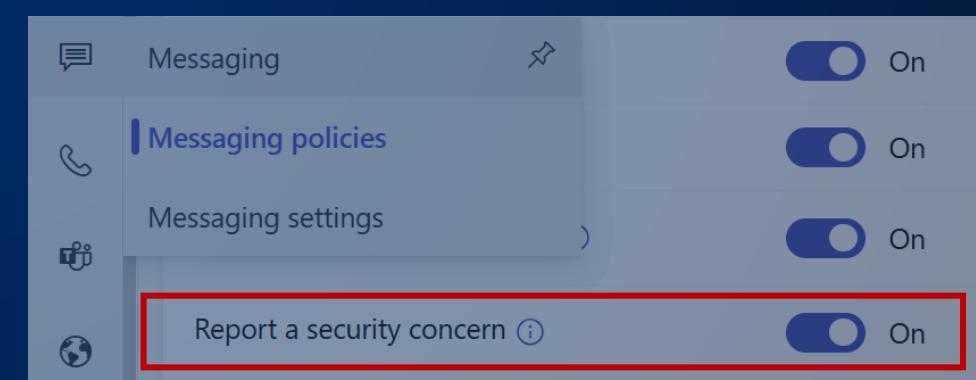
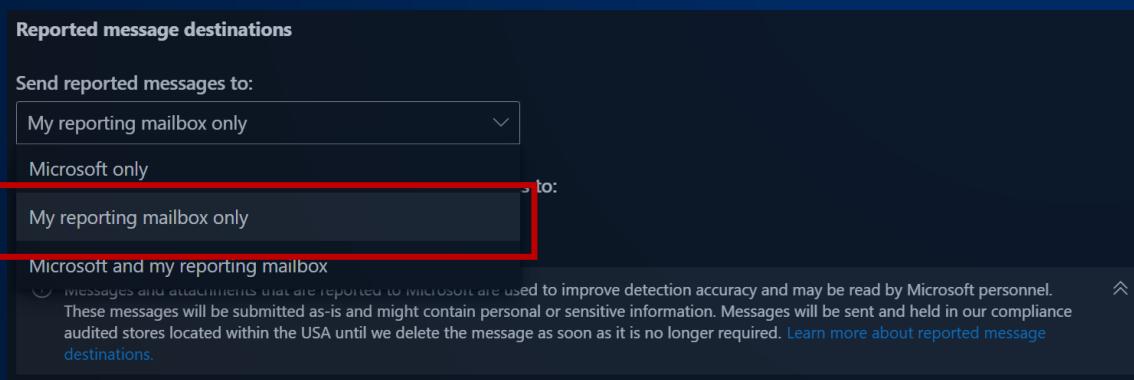
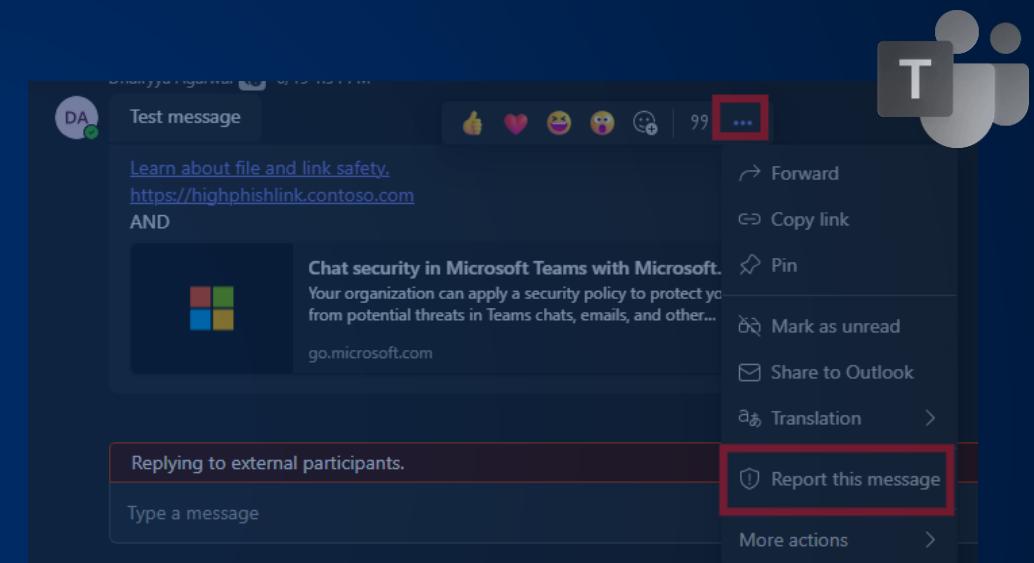
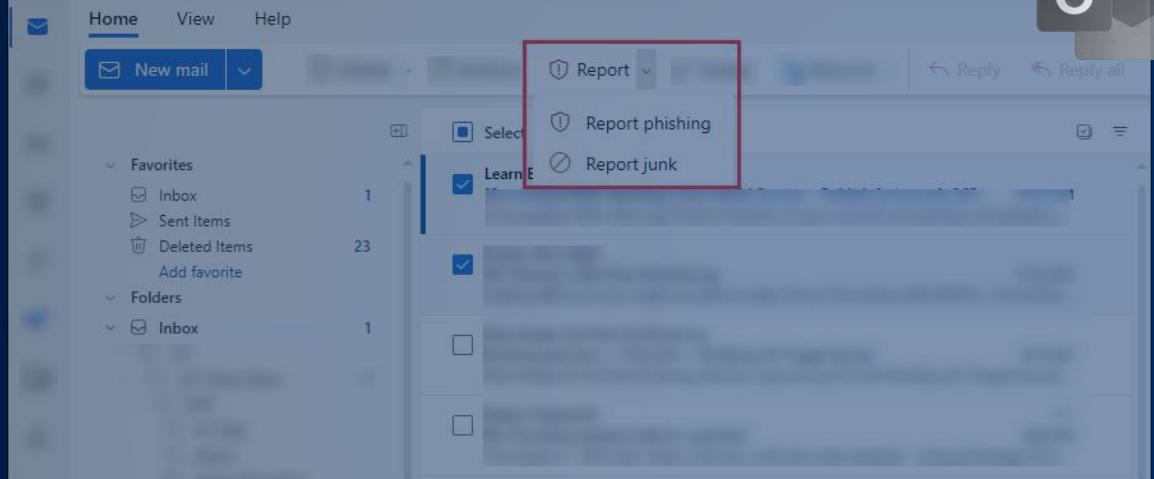


"Wonderlijk proces. Nooit zo meegemaakt"

"Ik dacht dat we klaar waren..."

"Strange, nietwaar?"

Rapporteer phishing mails!



Security = Right behavior + Technology

Dank voor jullie aandacht!

Slide deck is later terug te vinden op Github...



<https://github.com/DutchMSSecurityMeetup/slidedecks>