OUTKEPT

Ethical Phishing

De kracht van een community

Dieter Tinel

Co-founder @ OutKept

Cyber Security Consultant

Ethical hacker

brabantia

“Houd he rekening mee dat we vanaf vandaag een wijziging in onze bankrekeninggegevens hebben voor incaende betalingen. Voortaan moten all incoming betalingen have been overgemaakt naar onze filiaalrekening in Spanje. We het op prijs as u uw gegevens kunt bijwerken”

02 mei 2021

bol

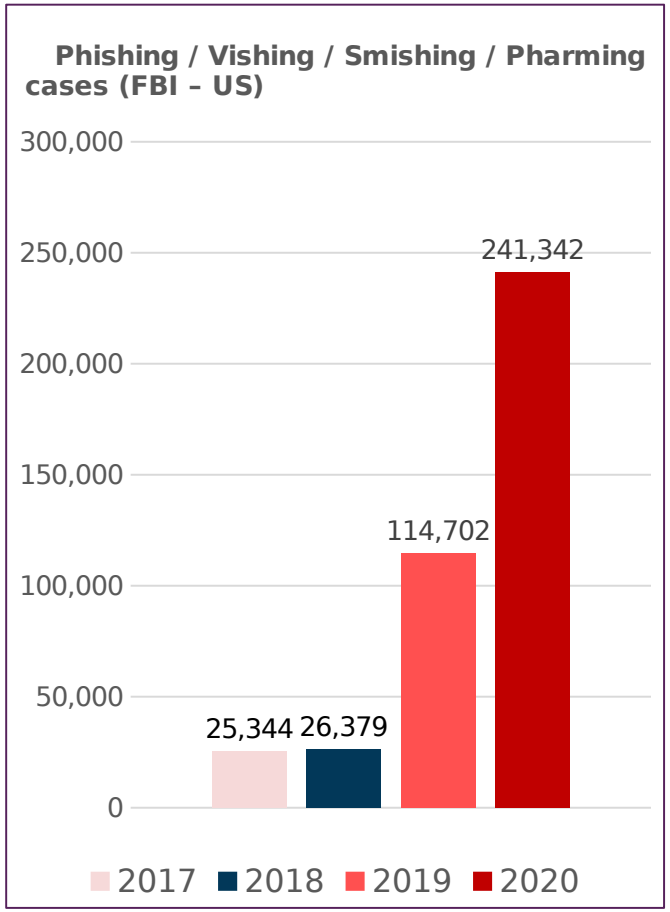
Ransomware aanval op Asco - 2019

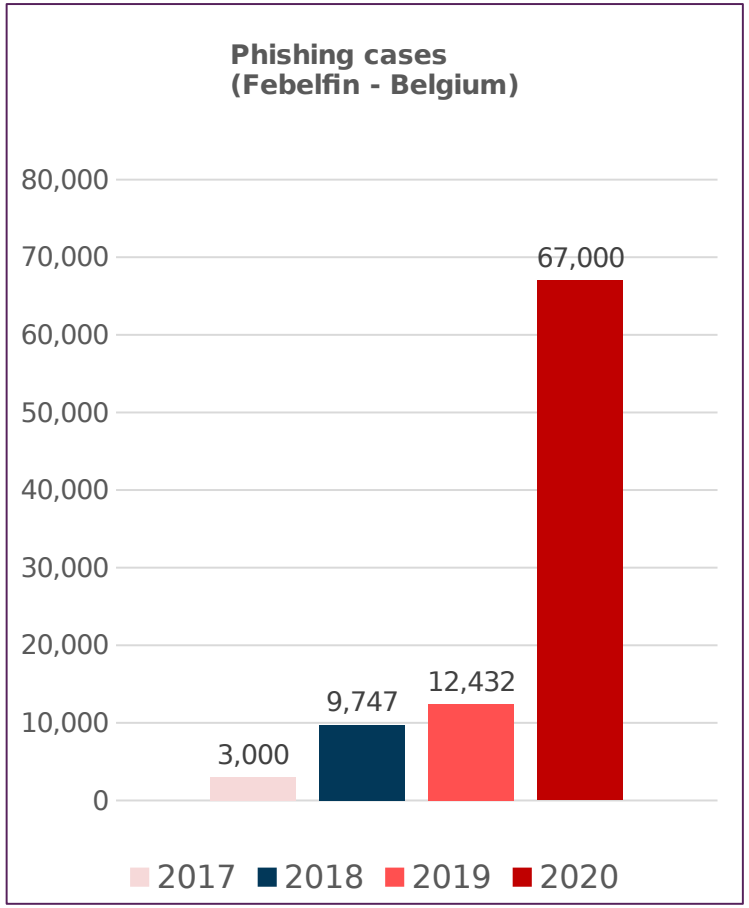
Kostenimpact van ~20 miljoen €

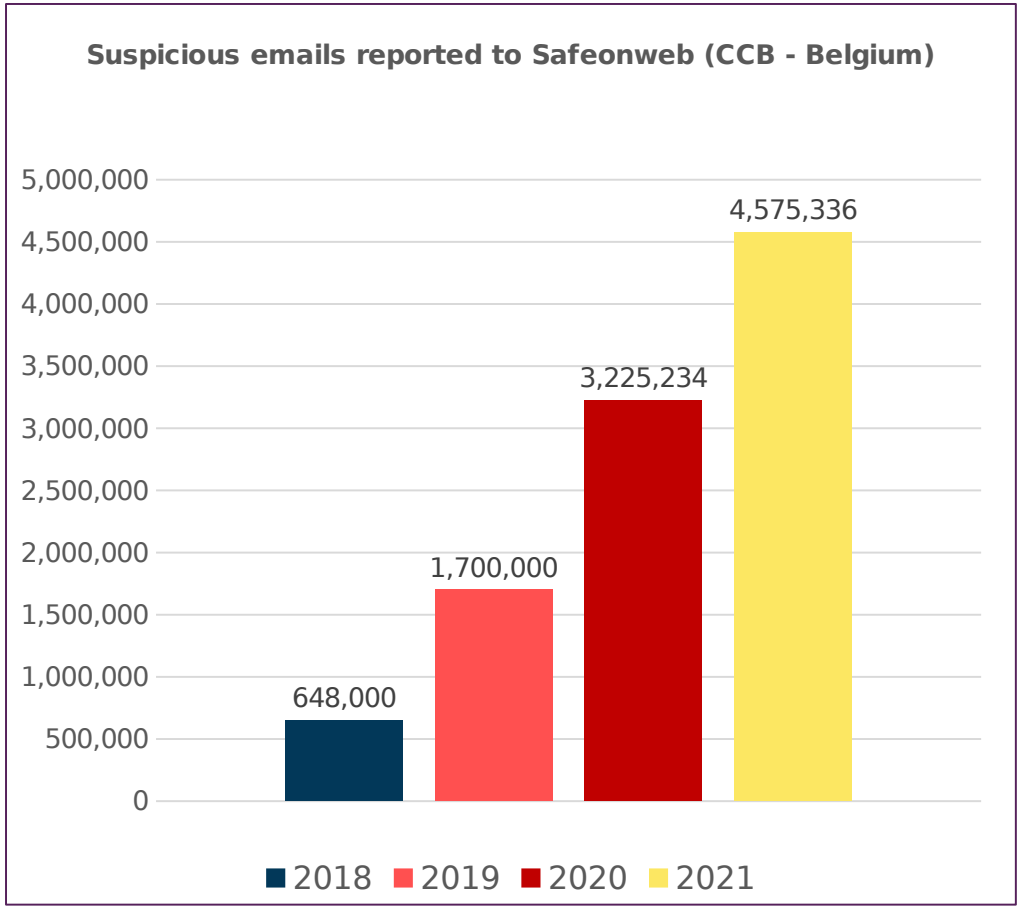
Ransomware aanval op Picanol - 2020

Kostenimpact van ~1 miljoen €

Phishing blijft volop groeien wereldwijd







Wat is phishing?

Bestaat uit het oplichten van mensen door ze te lokken naar een valse website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer.

Vorm van social engineering

Vaak aan begin van (reeks) misdrijven

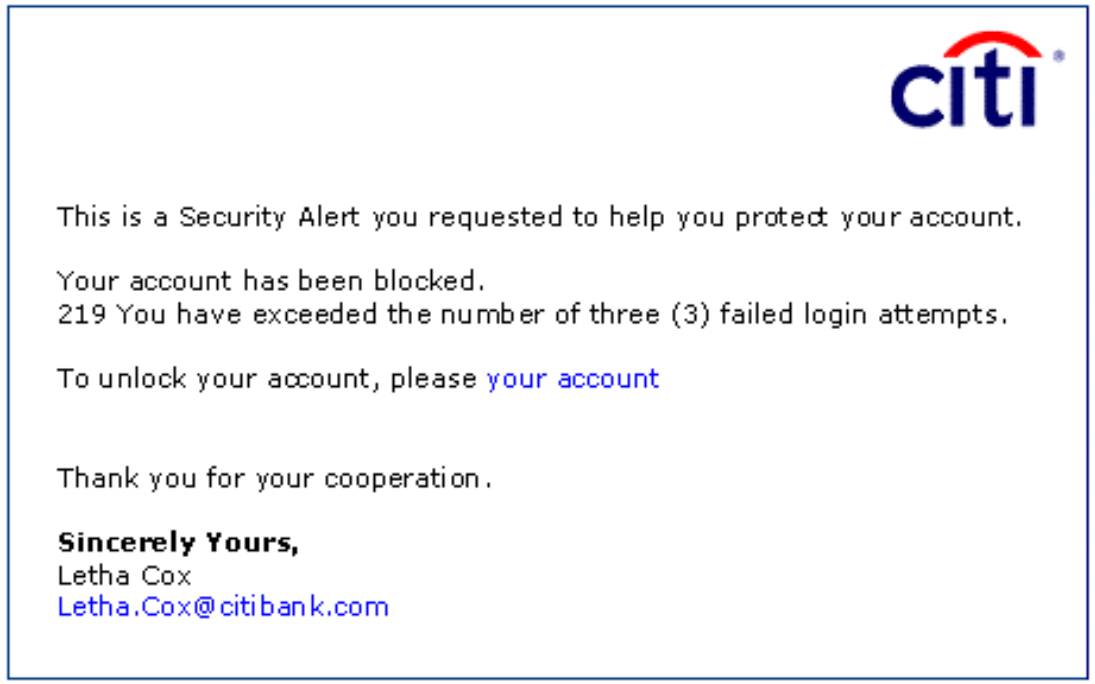
Analogie van phreaking

Experimenteren met telefoons, telefooncentrales, en andere telecomapparatuur

Spear phishing

Specifiek gericht op een individu, organisatie of bedrijf.

---------- Forwarded Message: ----------
From: "alerts@citibank.com" <ALERTS@CITIBANK.COM>
To: recipient@email.com
Subject: Security Alert: 06699
Date: Thu, 29 May 2008 12:41:41 +0000



Gedetailleerde kennis van de slachtoffers en hun contacten

Het gebruik van een echte persoon om betrouwbaarheid en geldigheid uit te stralen

De aanval is gericht op een klein aantal personen, waardoor het moeilijk te detecteren is

Cat phishing

Oplichting waarbij iemand zich voordoet als iemand anders

Kan leiden tot chantage

Probeert jouw vertrouwen te winnen / verliefd te maken

Slachtoffers schamen zich vaak

Sean Dhondt, Peter Van de Veire en Stan Van Samang. Beeld Qmusic, VRT, Belga

Is eigenlijk Gregory R. (27), de beelden zijn van de Instagram account van model Erin James. Hij maakte meer dan 12 slachtoffers en verspreidde de beelden samen met een vriend.

Na eerste gesprekken op Instagram verhuist de chat van platform en worden er pikante beelden uitgewisseld.

Ze dachten in contact te zijn met “**Eveline**”, die hen ertoe verleidt om foto’s te sturen.

Geschorst van St Lucas in Gent, na catphishen van mannelijke leerkrachten.

CEO Fraude / Whaling

Oplichting waarbij criminelen een onderneming contacteren met de vraag een belangrijke betaling uit te voeren naar hun bankrekening.

Nemen de identiteit aan van de CEO, CFO of een vertrouwd persoon

Populair in de zomermaanden

Misbruik van dringendheid

Clone Phishing

Kwaadaardige kopie van een – legitieme - eerder verzonden e-mail

De link of bijlage wordt vervangen

E-mail is vaak gespoofed zodat het lijkt te komen van de originele zender

Moeilijk te herkennen op basis van de inhoud

Vishing

Fraude waarbij oplichters slachtoffers via de telefoon proberen misleiden

Combinatie van de woorden 'voice' en 'phishing'

Oplichters proberen persoonlijke gegevens te achterhalen of geld te laten overmaken naar hen

Kunnen zich voordoen als een bankier, technicus, politieagent of als medeslachtoffer

Smishing

Oplichting waarbij men gevoelige gegevens via sms probeert te verkrijgen

Combinatie van de woorden 'sms' en 'phishing'

Er is haast bij

Afzender kan gespoofed zijn

Pharming

Fraude waarbij het verkeer van een website wordt gemanipuleerd

Hacker infecteert computer of server met malware dat DNS configuratie aanpast

De basisprincipes van het surfen op het internet worden misbruikt

Voorzorgsmaatregelen als checken van het webadres is niet voldoende

Evil twin aanval

Aanvaller zet een vals wifi access point op

Wifi naam is hetzelfde als de legitieme naam (evil twin)

Vaak bij publieke netwerken

Aanvaller zorgt voor sterker wifisignaal of is dichter bij de slachtoffers

Welke kanalen gebruiken phishers?

Welke technische maatregelen kan ik nemen?

- Spamfilter (*~45% e-mail is spam)
- Antivirus
- Security audit / pentest
- Netwerk segmentatie
- Beveiligde protocollen gebruiken (e.g. SSL/TLS, HTTPS, …)
- DNS correct configureren (DMARC, DKIM, SPF)
- Monitoring van kwaadaardige activiteiten

*Spam messages accounted for 45.37 percent of e-mail traffic in December 2021. Published by Statista Research Department, Jul 29, 2022

Waarom zijn technische maatregelen niet voldoende?

– Kan omzeild worden

– Kans op false positives of false negatives

– Alles dichttimmeren kan de workflow vertragen

– Mensen verliezen alertheid (wat als er toch nog iets doorgeraakt?)

– Phishers proberen je te bereiken via andere kanalen

Welke awareness maatregelen kan ik nemen?

- Workshops
- Video training
- Interactieve trainingen
- Phishing simulaties

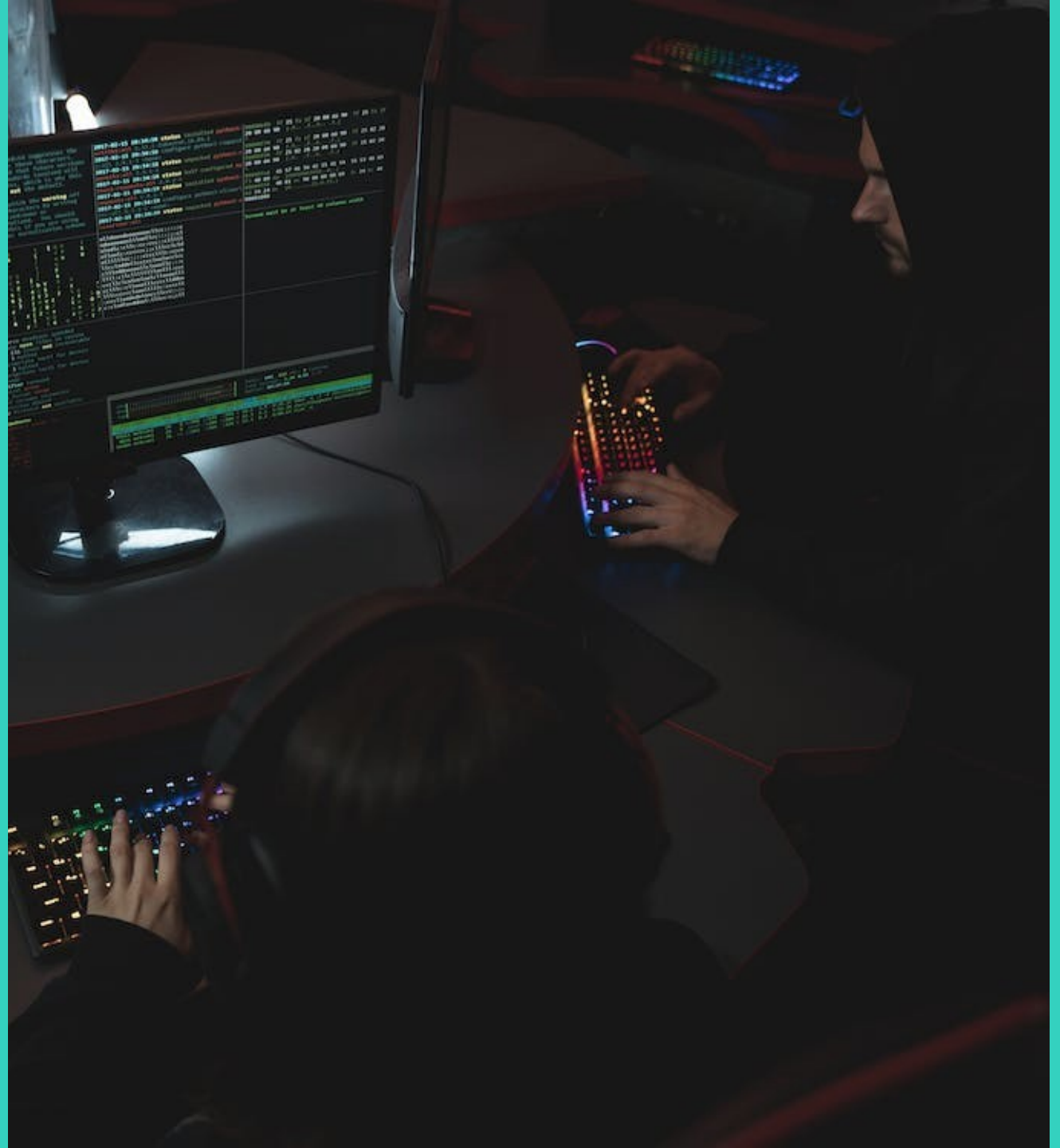
Wat zijn de nadelen klassieke awareness trainingen?

– Mensen vergeten wat ze tijdens de trainingen geleerd hebben

– Werknemers vinden de trainingen storend of tijdverlies

– Halen 100% op trainingen maar zijn nog steeds vatbaar voor de echte phishing mails

Wat is Ethical Phishing?



Hoe werkt ethical phishing?

Phishing e-mails gemaakt door ethische phishers

“Bounty” **rewards gebaseerd op succes**

(gamification)

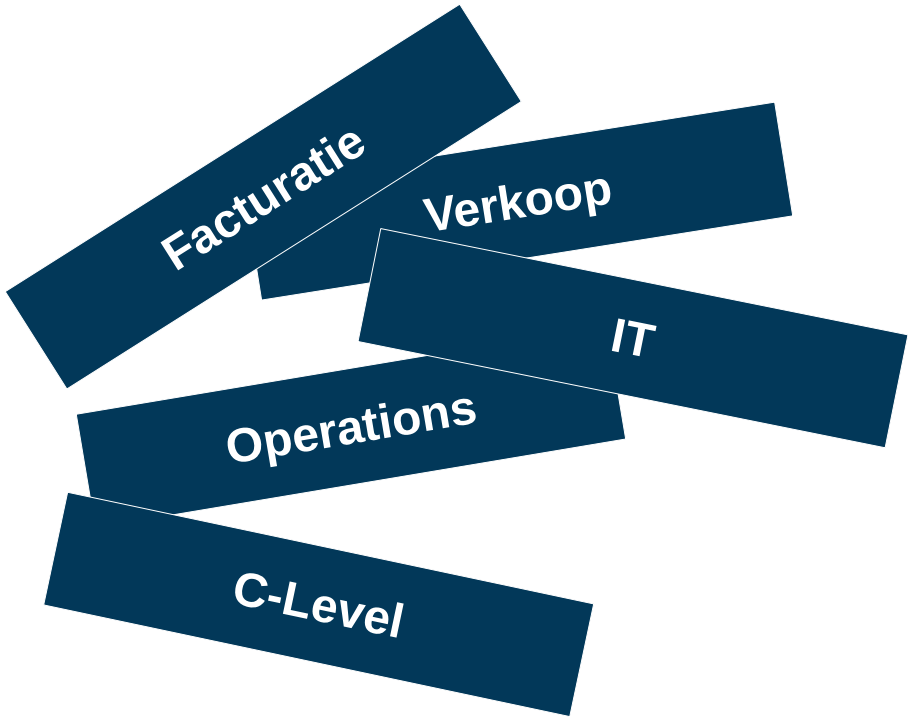
Kwaliteits- en veiligheidscontroles

Geautomatiseerde campagnes en realtime dashboard

Simulatiemails

Leerervaring via landing pagina’s, rapporteringen, enz.

Mogelijkheden voor spear phishing met behulp van tags and placeholders



“Hi {{Last name}} {{First name}},

your webmail account for {{Organisation Name}} has been compromised.

We have blocked your {{Department Name}} account for your own safety.

Kind Regards,
{{First name Colleague}}”

Wat is de motivatie van ethische phishers?

Mijn vrienden waren onder de indruk van mijn resultaten, en wilden het zelf ook proberen

Het is een gemakkelijk manier om wat extra te verdienen

Ik denk dat het cool is om te weten hoeveel mensen op mijn e-mails klikken; ik check het elke dag

Ik heb al redelijk wat geld verdiend met phishingmails deze maand

Wat zijn de voordelen van werken met ethische phishers?

- Kunnen inspelen op lokaal nieuws
- Expertise binnen bepaalde domeinen
- Competitieve onderscheiding
- Goedkoper

Een voorbeeld...

Vlaanderen
is zorg

Vaccinatiecentrum Gent
(Flanders Expo) - Gent

Persoonlijke uitnodiging derde vaccinatie

Beste {{Firstname}} {{Lastname}},

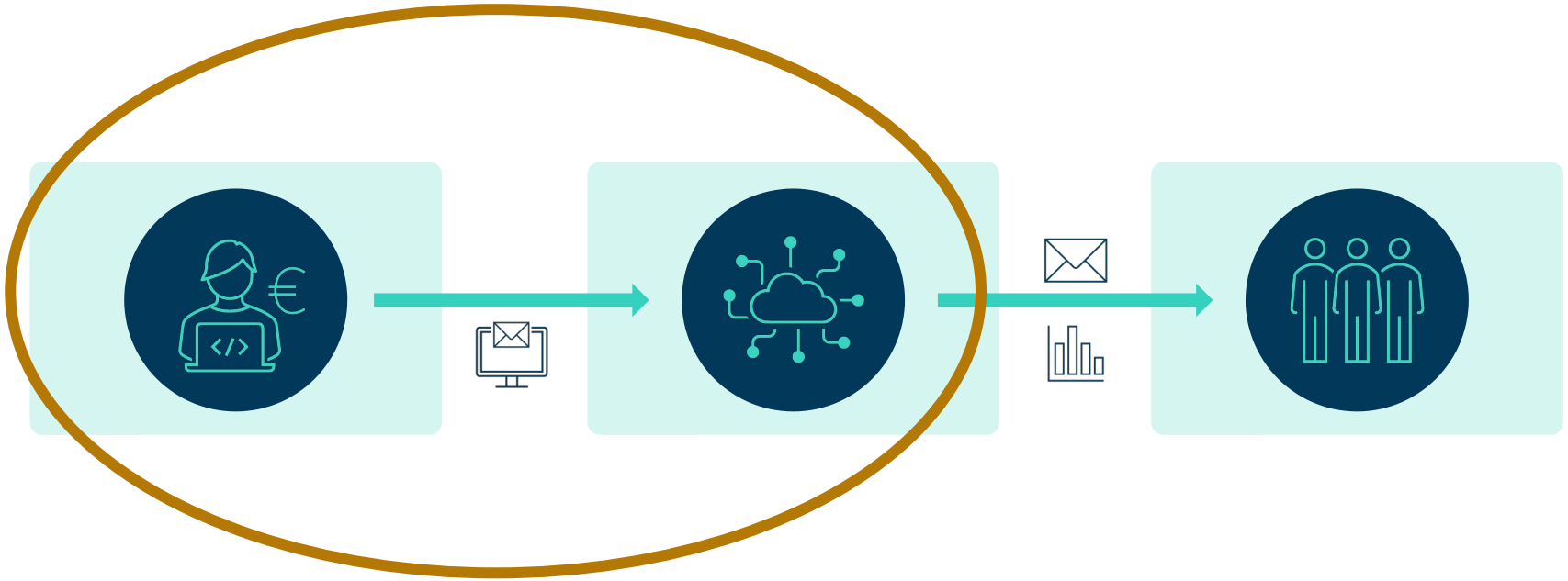
Op basis van de recent aangekondigde selectiecriteria, wordt u uitgenodigd voor een derde vaccinatie. Het betreft een optionele "booster" vaccinatie om het optimale bescherming te garanderen over een langere termijn.

Inschrijven?

- Indien u zich hiervoor wenst in te schrijven kan u dat doen hier

Vragen of meer informatie?

- Hiervoor kan u ook terecht op de inschrijvingspagina



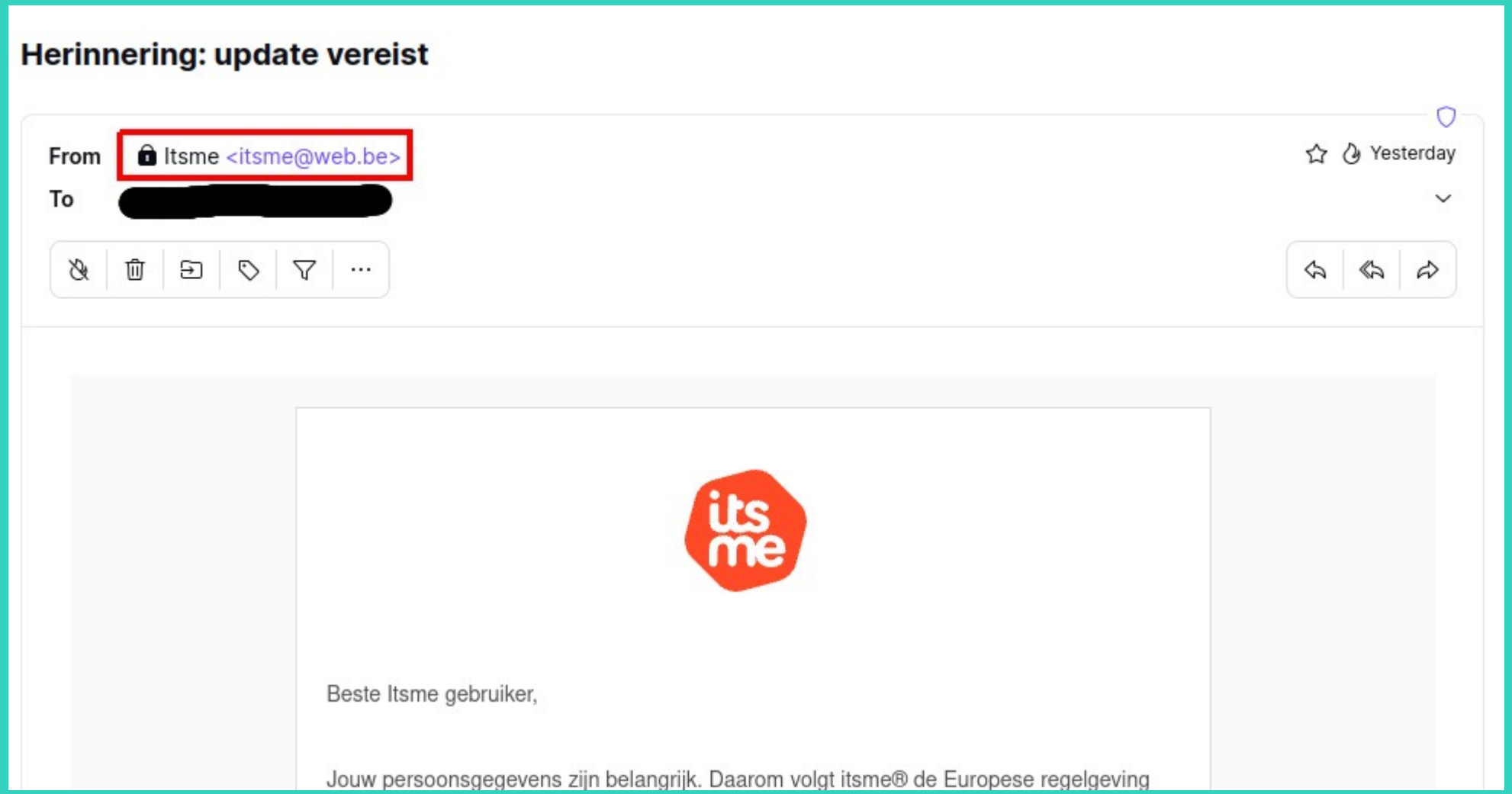
Een goed controlesysteem is onmisbaar

1. Elimineren van malafide templates

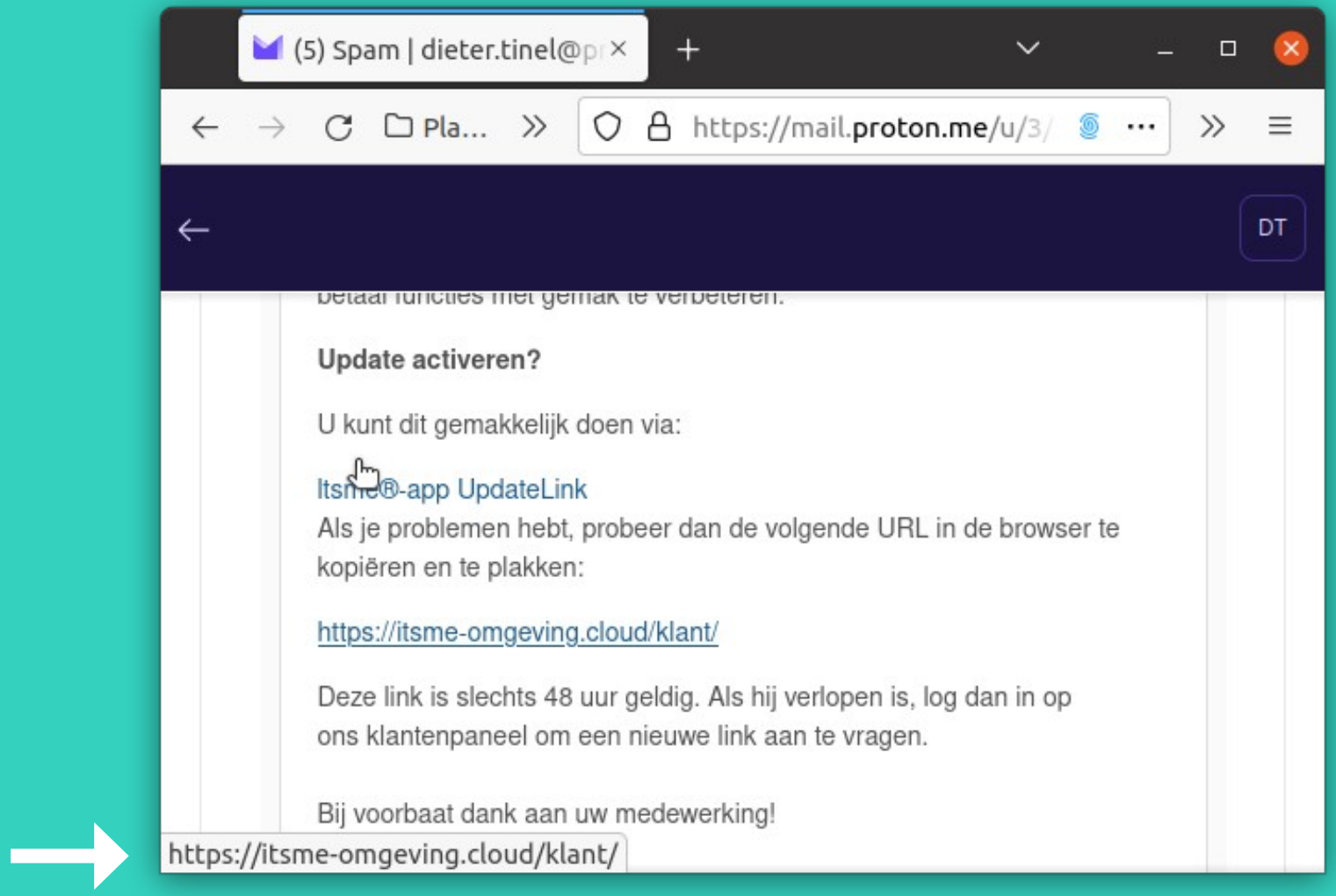
2. Anonimiseren van doelgroepen

Hoe kan ik phishing herkennen?

1. Check de afzender



2. Controleer de link



3. Taalgebruik of vormgeving

DigiD

Geachte heer/mevrouw,

Verouderrd

Uwe digitale sleutel voor toegang tot uw DigiD is verouderd. Aktiveer uw sleutel voor 28-11-2022 om deaktivatie te voorkomen via onze site: DigiD.nl/Verifieren

4. Spoed of urgentie

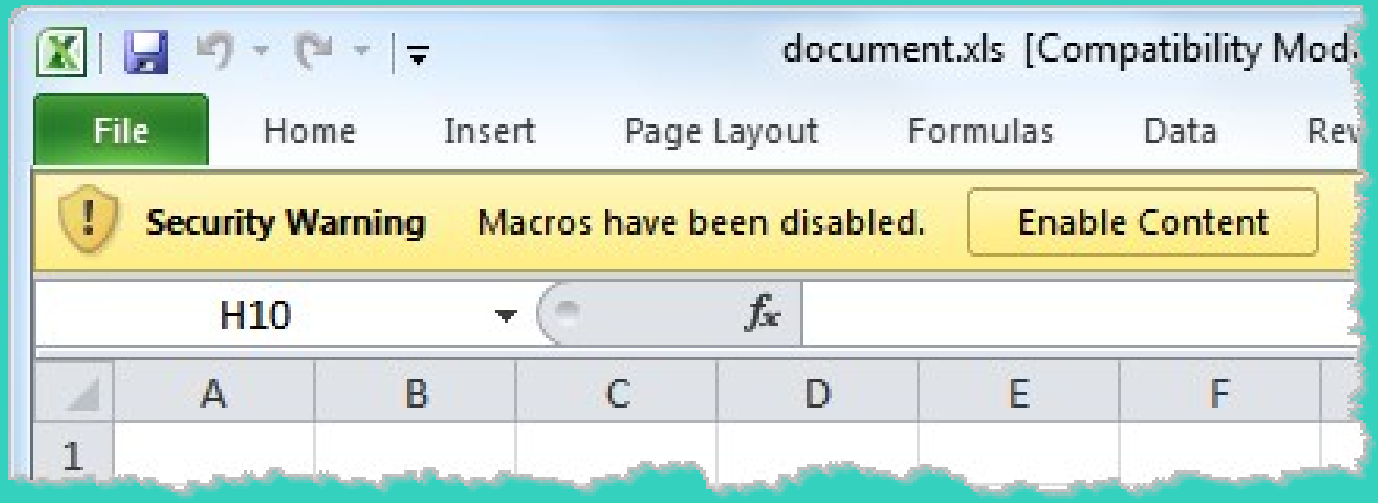
Contróleer uw gegevens

Indien UBO's niet tijdig worden geregistreerd kunnen hierdoor flinke boetes verschuldigd worden. De maximale bestuurlijke boete voor he overtreden van de regels met betrekking tot het UBO-register bedraa op dit moment € 2.500 (dit bedrag kan jaarlijks wijzigen). Daarnaast k ook een last onder dwangsom worden opgelegd, waardoor de maxim boete hoger kan uitvallen. Voorkom deze boetes en maak de UBO tij kenbaar.
Alvast hartelijk dank voor uw medewerking.
Met vriendelijke groet,

Kamer van Koophandel

5. Onverwacht verzoek van een gekende

6. Bijlages

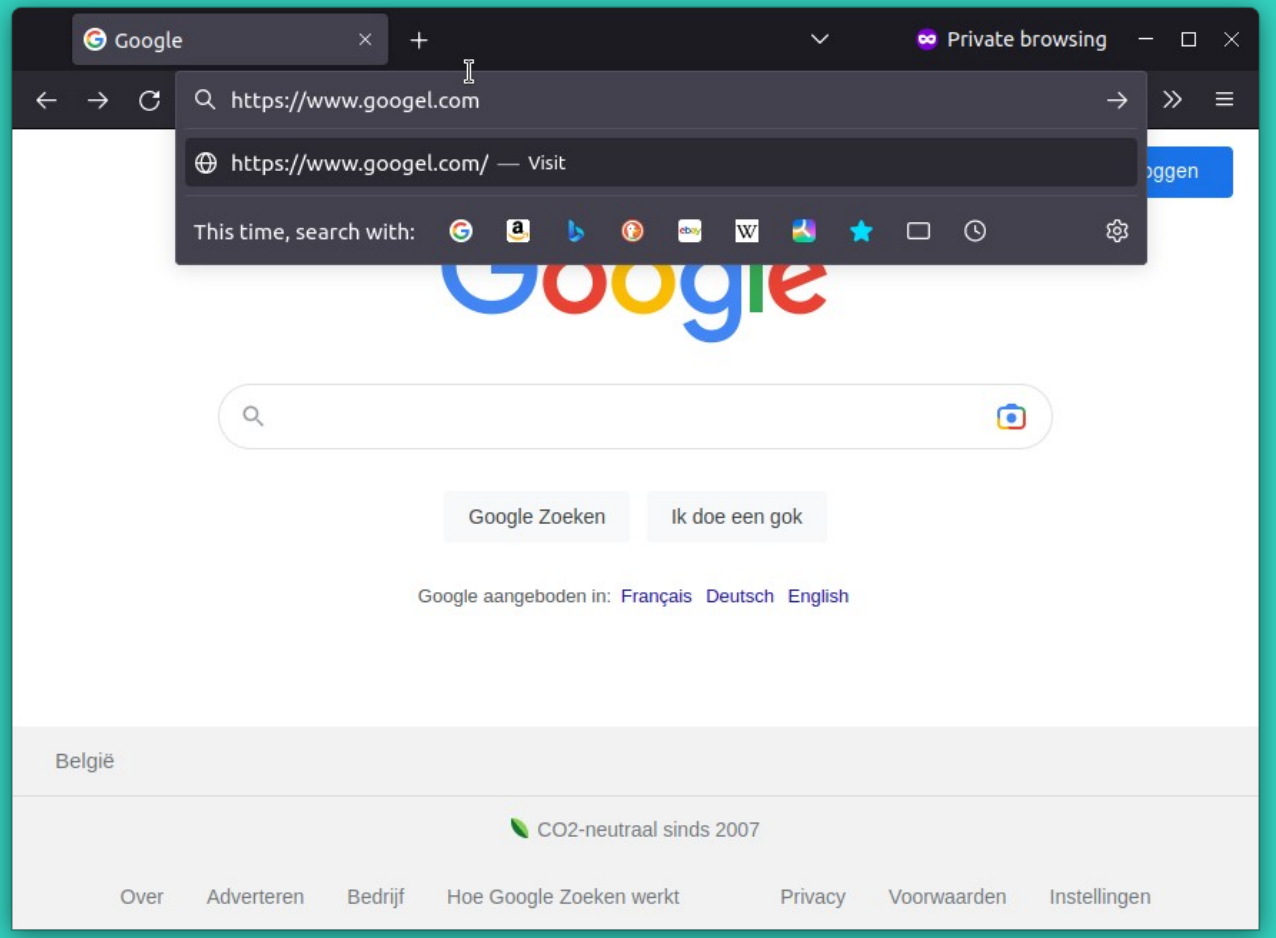


.exe .cmd .bat

.docm .bin

.html .sh

7. Typosquatting



Test jezelf!

Wat is hier het secondleveldomein?

www.google.com

Wat is hier het secondleveldomein?

~~www.~~google.com

Wat is hier het secondleveldomein?

www.faceb00k.com

Wat is hier het secondleveldomein?

~~www.~~faceb00k.com

Not ‘facebook’

Wat is hier het secondleveldomein?

www.apples.com

Wat is hier het secondleveldomein?

~~www.~~apples.com

Not ‘apple’

Wat is hier het secondleveldomein?

www-microsoft.org

Wat is hier het secondleveldomein?

www-microsoft.org

Not bad…

… let's make it harder

Wat is hier het secondleveldomein?

https://pixabay.com/en/photos/?hp

Wat is hier het secondleveldomein?

~~https://~~pixabay.com~~/en/photos/?hp~~

Wat is hier het secondleveldomein?

https://youtube.com.profile.online/video/Epld51

Wat is hier het secondleveldomein?

~~https://youtube.com.~~profile.online~~/video/Epld51~~

Top level domain

Wat is hier het secondleveldomein?

https://www.amazon.com/s/ref=br_pdt_mgUpt

Wat is hier het secondleveldomein?

~~https://www.amazon.com/s/ref=br_pdt_mgUpt~~

Not ‘amazon’

Wat is hier het secondleveldomein?

~~https://www.amazon.com/s/ref=br_pdt_mgUpt~~

? Niet ‘amazon’ ?

? ? ? ?

Wat is hier het secondleveldomein?

~~https://www.amazon.com/s/ref=br_pdt_mgUpt~~

xn—mazon-3ve.com

Not the same ‘a’
Cyrillic / Latin

Ook wel homograph / punnycode aanval genoemd

Welke andere maatregelen kan ik nemen?

1. Zorg voor een degelijk wachtwoordbeleid

– Verander je belangrijkste wachtwoorden regelmatig

– Maak je wachtwoorden complex

– Gebruik nooit hetzelfde wachtwoord

– Maak gebruik van een wachtwoordmanager

– Schakel multi-factor authenticatie in

– Deel je wachtwoorden met niemand (ook niet met familie, vrienden, of beste collega’s)

– Check of je e-mail deel is van een datalek: https://haveibeenpwned.com

2. Maak back-ups van je bestanden

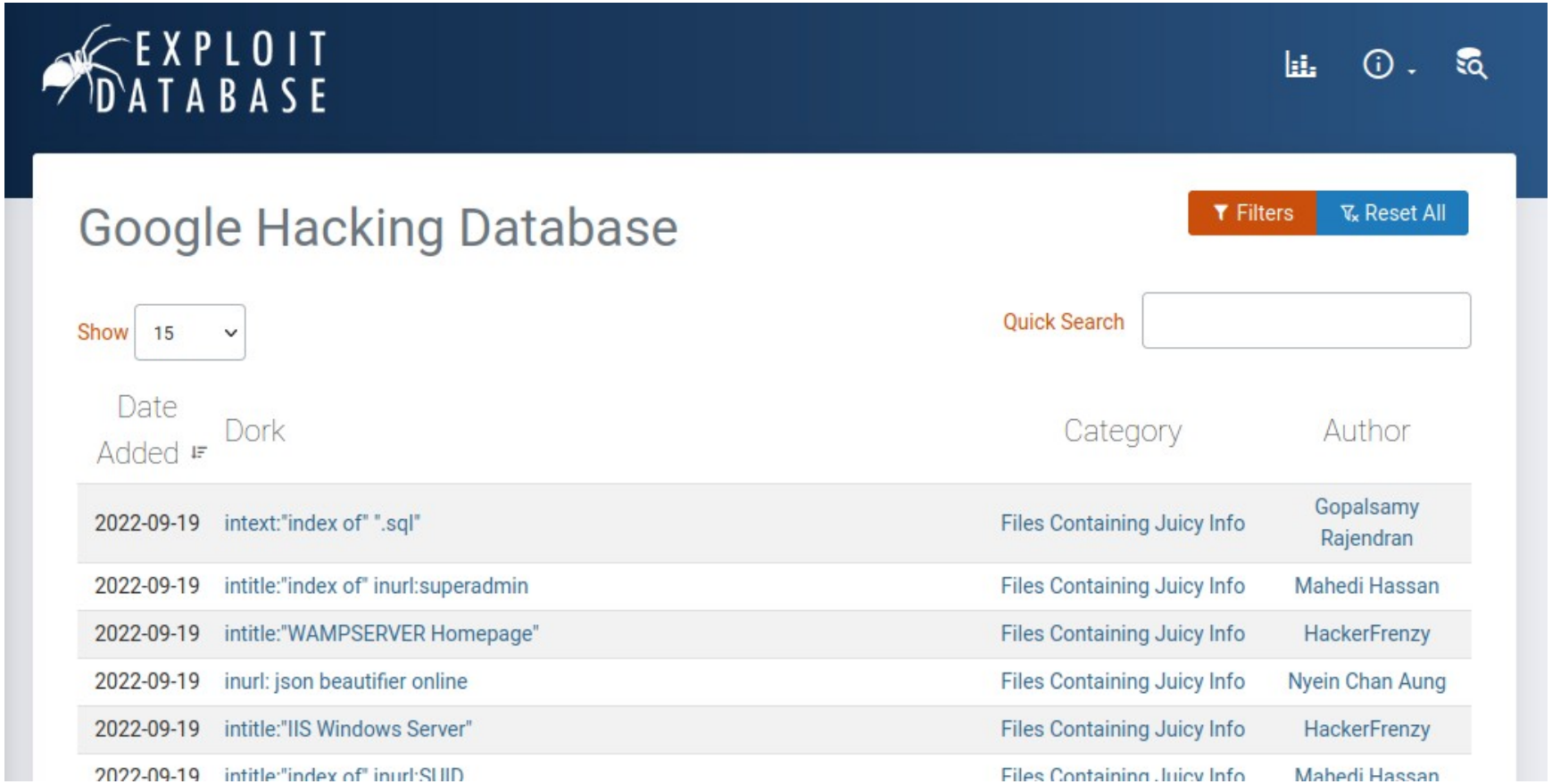
– Een niet geteste back-up is geen back-up

– Bewaar je back-ups op 2 of meerdere plaatsen

– Zorg ook voor offline back-ups

– Gebruik versioning indien mogelijk

3. Let op met wat je online zet

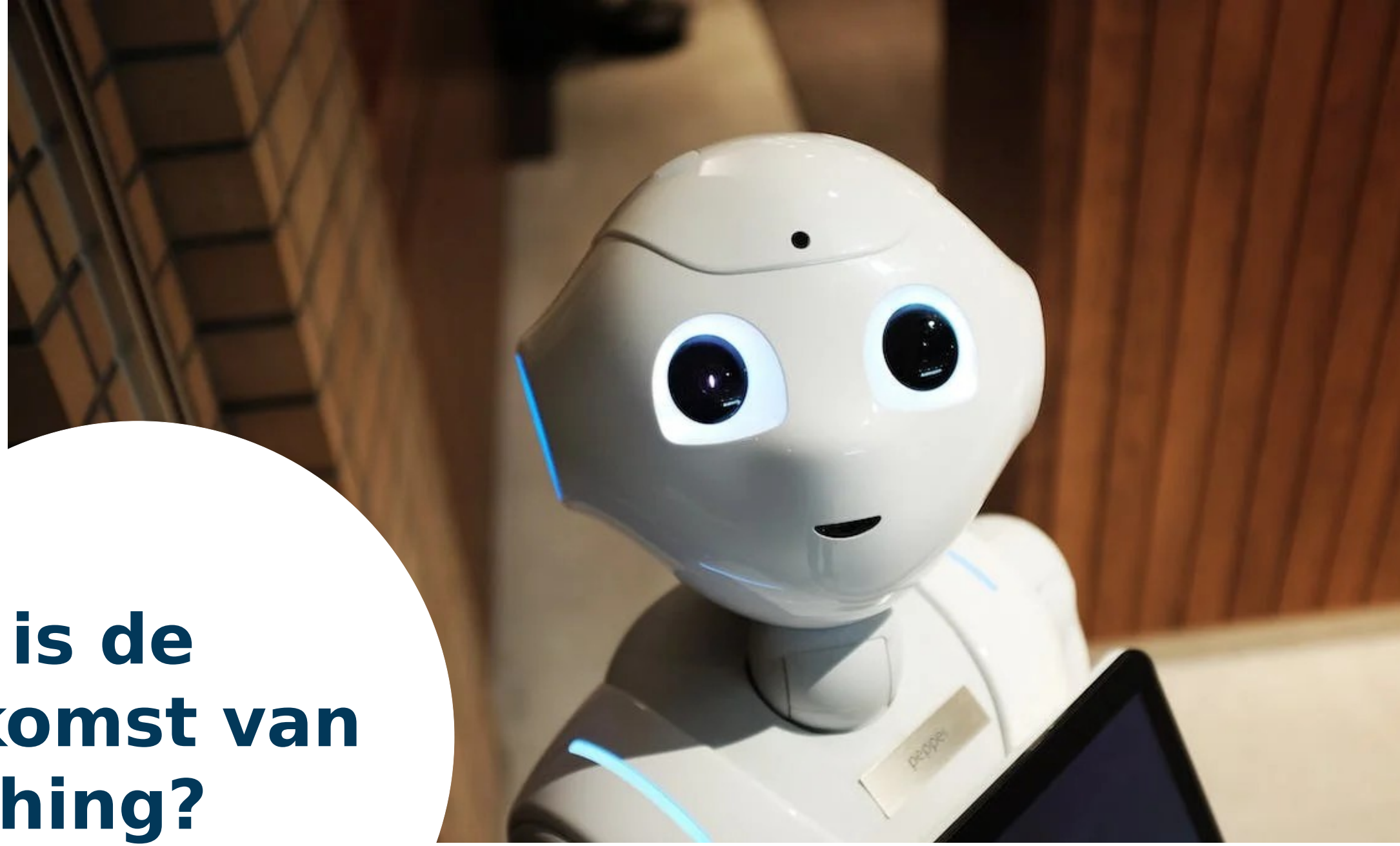


Phishers zoeken online naar gevoelige gegevens of kenmerken die meer vertrouwen kunnen wekken

4. Doe regelmatig updates

- Besturingssystemen
- Browser
- Smartphone
- E-mail software / office
- Antivirus
- ...

Wat is de toekomst van phishing?



Gebruik van AI voor het genereren van phishingmails

State-sponsored cyber attacks

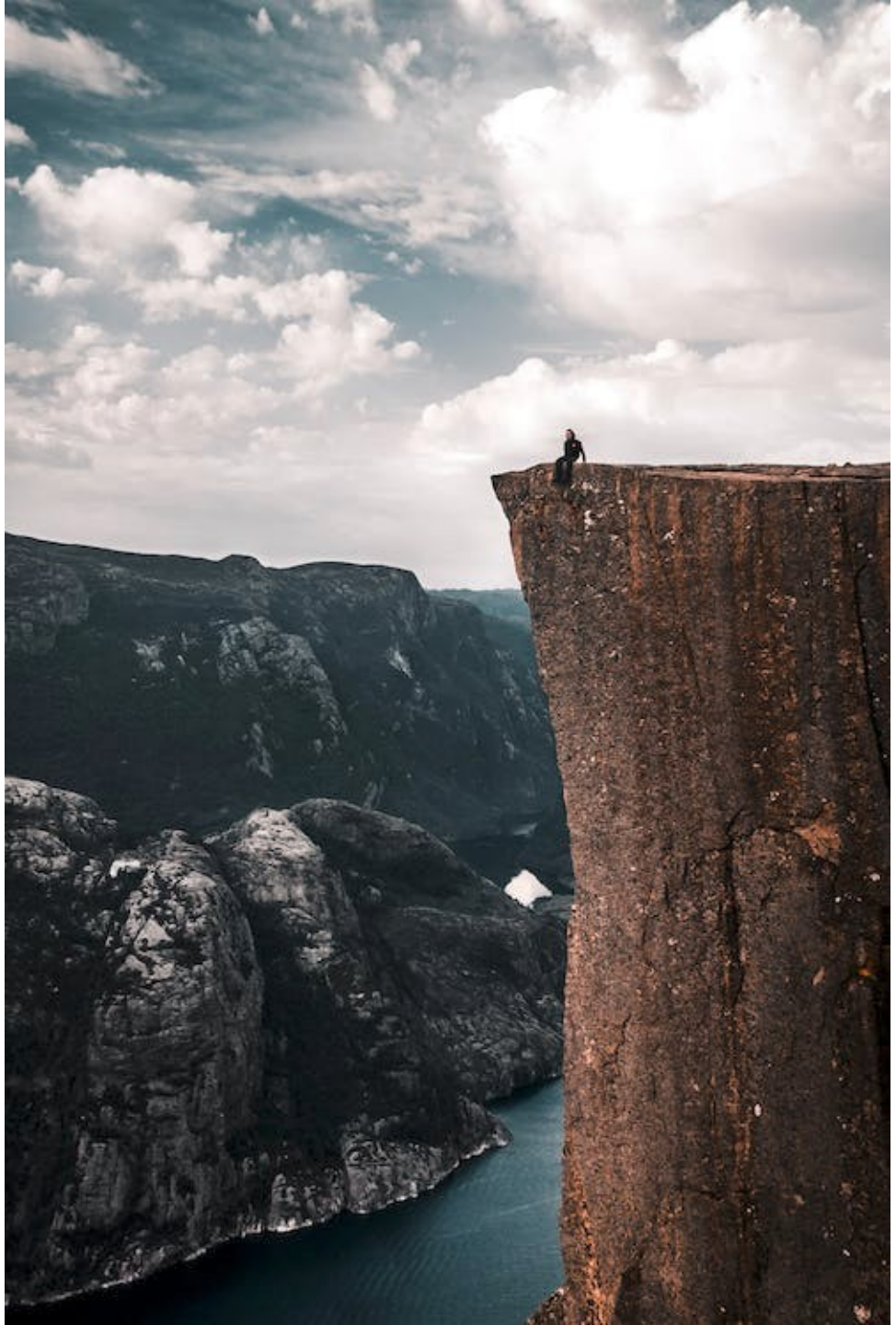
Metaverse

Deepfakes

Gebruikt van AI voor het detecteren van phishing mails

Dieter Tinel
E: dieter.tinel@outkept.com
T: +32 470 66 95 01

Bedankt voor uw aandacht



Stay safe!