

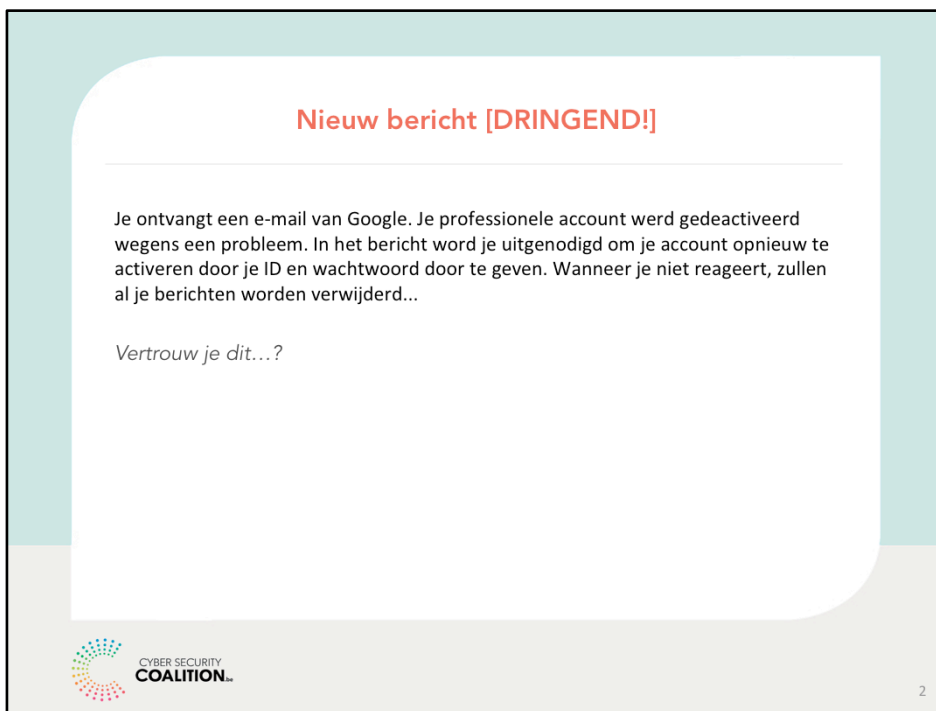


Laat je niet beetnemen

Bescherm je tegen phishing berichten

Brussel, juli 2020

Hallo en welkom allemaal!



Het klassieke phishing-scenario bij kmo's.

Case1: Universiteit Maastricht

Op 15 en 16 oktober 2019 heeft een hacker toegang gekregen tot het netwerk van Universiteit Maastricht doordat 2 medewerkers op het attachment in een mail hadden geklikt. Van 16 oktober tot 23 december heeft de aanvaller verschillende servers gecompromiteerd. Op 21 november is de aanvaller erin geslaagd om via een server met ontbrekende veiligheidsupdates volledige rechten te verwerven binnen de infrastructuur van de universiteit. Op 23 december heeft de aanvaller op 267 Windows server een ransomware (gijzelingssoftware : de hacker versleutelt gegevens en in ruil voor losgeld wordt alles weer ontsleuteld) uitgerold. Na zorgvuldige analyse - het lekken van waardevolle research data en info over commerciële operaties stond op het spel - besliste de universiteit op 30 december het gevraagde losgeld van 220.000 USD te betalen.



3

De case van de Universiteit van Maastricht (bron: FOX IT – NCC Groep) toont aan dat hackers tijd hebben, grondig te werk gaan, onder de radar kunnen blijven.

Het incident leidde tot volgende aanbevelingen van de betrokken veiligheidsconsulenten:

- Verbeter processen omtrent vulnerability & patch management
- Breng meer segmentatie aan binnen de netwerk architectuur en gebruikersrechten
- Implementeer of verbeter netwerk- en logmonitoring
- Oefen planmatig met verschillende crisis scenario's en verbeter de opgestelde plannen waar nodig

Case2: Picanol

Op 15 januari 2020 kreeg weefgetouwenproducent Picanol België het nieuws dat Chinese collega's niet konden inloggen op een aantal IT-systemen. Ook in de moedervestiging in Ieper waren er al problemen. Na een week inactiviteit kon de productie geleidelijk aan weer opgestart worden. Oorzaak was een malware-aanval; er werd ook losgeld gevraagd, maar Picanol betaalde niet. Picanol raamt de schade op 'minder dan 1 MIO EUR'.



Bron: VRT Nieuws (Januari 2020)




Opgepast: phishing!

Een persoon met slechte bedoelingen wil informatie te pakken krijgen.

In je professionele inbox, je vertrouwelijke dossiers, je online-accounts, ... Vaak stopt het niet daar en gaat men ook aan de haal met heel wat informatie van je profiel op de sociale netwerken en doet men aankopen op je favoriete sites.

Phishing

is een veel gebruikte techniek die steeds meer geperfectioneerd wordt



Phishing... wasda?

Phishing:

- 'Hengelen'
- Identiteit stelen
- Misbruik van vertrouwen
- E-mail, SMS (Smishing), WhatsApp, Messenger, ...
- Phishing via telefoon (Vishing)

Doel:

- Persoonlijke informatie
- Gevoelige gegevens van de onderneming
- Geldtransfer
- Industriële sabotage

Hoe?

- Besmette bijlage
- Link naar valse website
- Vals betalingssysteem

Phishing, afgeleid van het Engelse woord voor **hengelen**, is een frauduleuze techniek waarbij **de identiteit van een persoon of instelling wordt gestolen**.

De fraudeur doet het slachtoffer geloven dat hij of zij zich tot een **betrouwenswaardige partij** richt – een bank, administratie, persoonlijke contactpersoon, ... — om **persoonlijke of professionele informatie** los te krijgen.

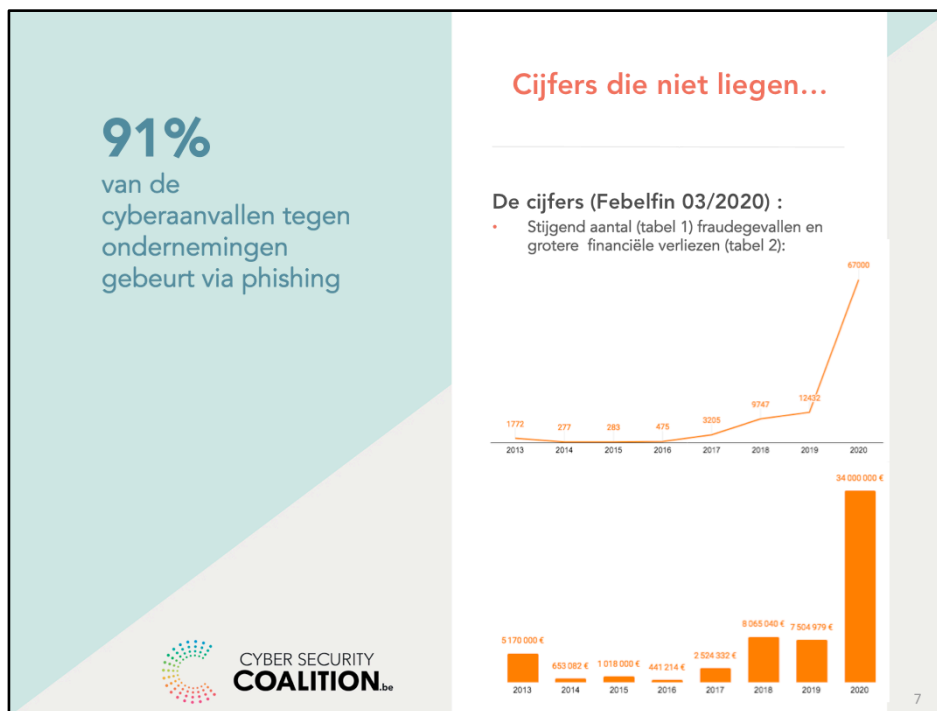
Meestal gebeurt dit via een **e-mail**, maar ook via **SMS (Smishing), WhatsApp, Messenger, ... Ook via telefoon (Vishing, V= voice)**

De bedoeling?

- Het verzamelen van **persoonlijke informatie** (ID, wachtwoord, kredietkaartnummer).
- Toegang verkrijgen tot **gevoelige gegevens** binnen de onderneming.
- Een **geldtransfer** verkrijgen.
- Industriële **sabotage**.

Hoe?

- Een **besmette bijlage** die een virus installeert.
- Een link die je doorstuurt naar een **valse website**.
- Een vals **betalingssysteem**.



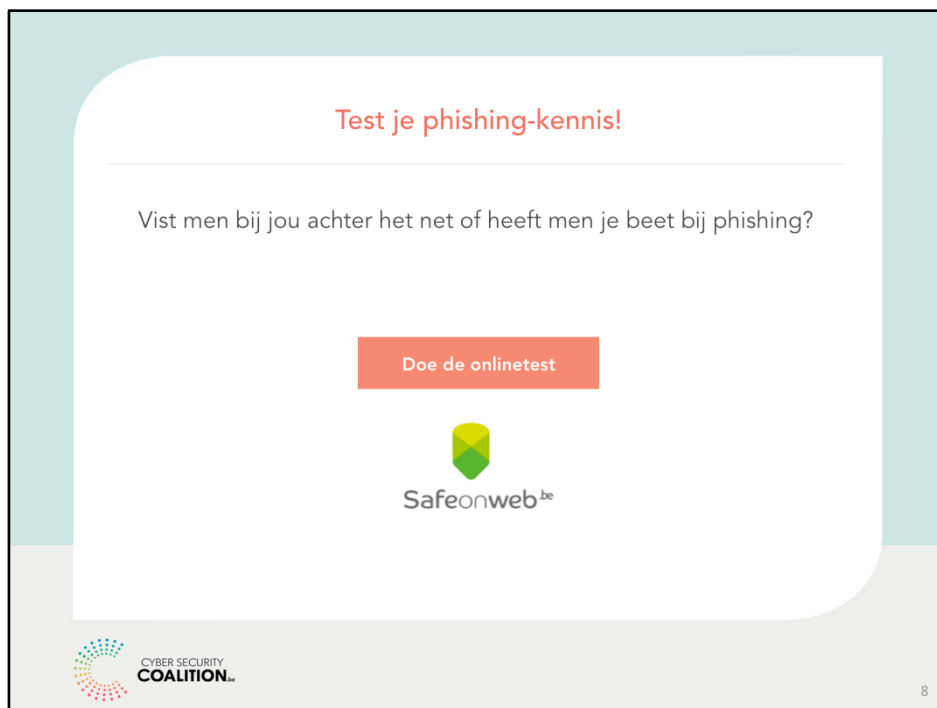
Phishing vertegenwoordigt **91% van alle cyberaanvallen tegen bedrijven** (Cert – 2015)

Unizo (**Unie** Zelfstandige **O**ndernemers in Flanders) stelde in 2018 dat 1 Belgische onderneming op 5 al slachtoffer was van dit type van fraude.

Aantal fraudegevallen en financiële verliezen in de financiële sector in België (bron: Febelfin – maart 2020): het aantal geslaagde fraudegevallen via phishing is in 2019 (12.432) opnieuw sterk gestegen met 27,5% in vergelijking met 2018 (9.747). De kost van deze fraudegevallen voor de Belgische financiële instellingen lijkt gestabiliseerd in 2019 (7,5 MIO EUR) ten opzichte van 2018 (8 MIO EUR). Een rekensom leert dat cybercriminelen in 2019 gemiddeld 604 euro per slachtoffer buit maakten. In veruit de meeste gevallen gaat het om kleine bedragen maar soms worden ook grote sommen buit gemaakt. Helaas gaan de cijfers begin 2020 (Covid-19) opnieuw zeer sterk de hoogte in.

Dankzij de massale hulp van de Belgische bevolking kon het Centrum voor Cybersecurity Belgium (CCB) in 2018 gemiddeld **4 frauduleuze websites per dag** blokkeren. In totaal werden zo **1478 valse websites geblokkeerd**.

In 2018 stuurde de Belgische bevolking **648.522 mails** door naar verdacht@safeonweb.be. De doorgestuurde mails worden automatisch gescand door onze software, die de naam BeFish kreeg. In een eerste fase worden de berichten met URL's geïdentificeerd. Daarna detecteert de anti-virustechnologie verdachte links in deze mails, die worden doorgestuurd naar *EU Phishing Initiative*. Deze laat de phishing websites blokkeren via een samenwerking met 4 browsers: Google Chrome, Mozilla Firefox, Safari en Internet Explorer.



Afspraak op: <https://www.safeonweb.be/nl/quiz/phishingtest>

In deze **(anonieme) test** zal je **10 e-mails** zien die worden verstuurd door echte ondernemingen en organisaties en door fraudeurs.

- Kan jij de phishing-e-mails **ontmaskeren**?
- Daag je collega's uit: wie behaalt de **beste score**?

Je zal zien dat het **niet altijd makkelijk is**. Maar geen paniek, oefening baart kunst...

Waakzaam zijn

Gebruik je gezond verstand en wees voorzichtig!



Hoe een phishing-e-mail ontmaskeren?

De signalen:

- Vreemde boodschap
- Vaag onderwerp
- Spam
- Alarmerende toon

9

Ontmasker een phishing-e-mail

- Er is **geen enkele reden** waarom je dit bericht zou ontvangen.
- Het onderwerp van de e-mail blijft **vaag**, je haalt de context er niet uit.
- Hij is in je **spam** beland.
- De toon is **alarmerend**, bedreigend of intrigerend.

2 weten meer dan 1

In geval van twijfel,
praat erover met
anderen



Wat doen bij phishing?

De reflexen:

- Niet antwoorden
- Controleer adres verzender (Hover over de afzender zodat het volledige e-mailadres zichtbaar wordt)
- Check betrouwbaarheid links (Hover over de link zodat het webadres dat erachter zit zichtbaar wordt)
- Opgepast voor bijlages
- Gebruik geen onbekend betalingssystemen

10

Neem de juiste reflexen aan bij phishing

- **Beantwoord** de e-mail **niet**!
- Controleer de correctheid van het **adres van de verzender**: Hover over de afzender zodat het volledige e-mailadres zichtbaar wordt. De 2 laatste woorden achter @ en voor de eerste enkele '/' geven het domein van het bedrijf weer. Controleer of dit overeenstemt met het officiële domein van dit bedrijf.
- Overloop de links om de **betrouwbaarheid ervan na te gaan**: Hover over de link zodat het webadres dat erachter zit zichtbaar wordt. De 2 laatste woorden voor de eerste, enkelvoudig slash geven het domein van het bedrijf weer. Controleer of dit overeenstemt met het officiële domein van dit bedrijf.
- Wantrouw **bijlages**, bestanden en afbeeldingen.
- Doe **geen transacties** via een onbekend systeem of een ander dan gebruikelijk betalingssysteem, of via een gewijzigd rekeningnummer (check!).

Geen paniek

Waarschuw
onmiddellijk de
verantwoordelijke



Hoe reageren bij een aanval?

De middelen:

- Contact via ander kanaal
- Verantwoordelijke
- Wachtwoorden
- Back-ups
- Antiviruscontrole

11

Reageer bij een phishing-aanval

- Contacteer **via een ander kanaal** de persoon of organisatie.
- Waarschuw de **verantwoordelijke** binnen je onderneming.
- Wijzig je professionele en privé**wachtwoorden**.
- Bewaar je **gegevens op een veilige plek** en maak een back-up.
- Voer een **antiviruscontrole** uit op je computer.

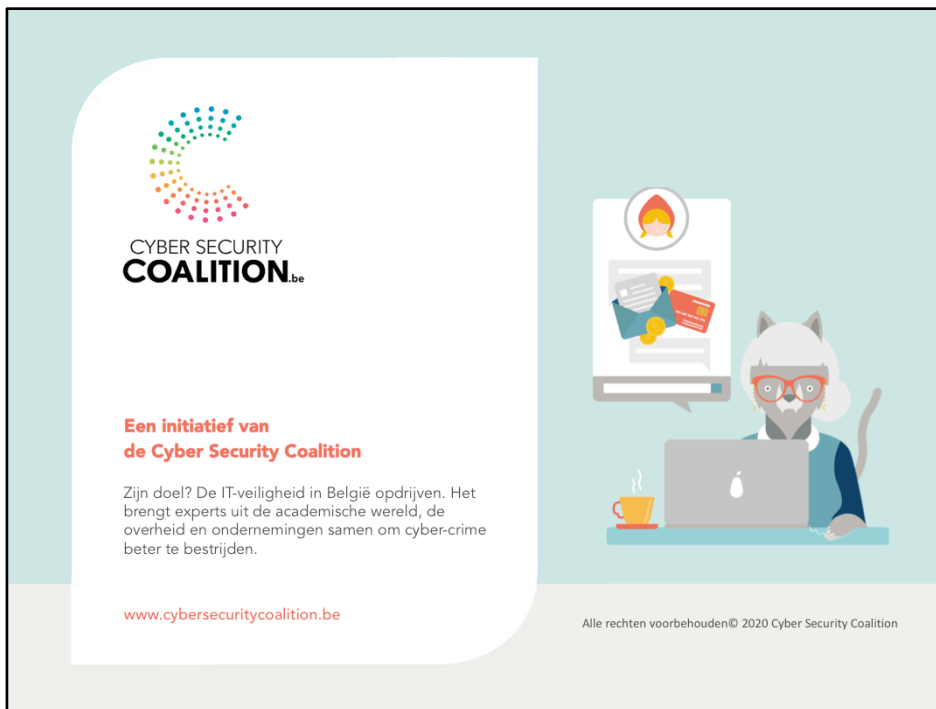
Phishing: praat erover!

Wat is jouw mening?
Heb je opmerkingen?
Wat heb je
onthouden?
Je eerste actie?



12

Wat is jouw mening?
Heb je opmerkingen?
Wat heb je onthouden?
Wat zal de eerste actie zijn die je onderneemt na deze presentatie?



Bedankt voor je aandacht!