Les 2: Trap er niet in! (Phishing)

Les 2: Trap er niet in! (Phishing)

1. Wat is Phishing?

In Les 1 leerden we over "Brute Force": het raden van wachtwoorden. Deze les gaat over **Phishing**: een poging om je te lokken (vissen) zodat je zelf je gegevens geeft .

Het is psychologisch manipuleren van de mens. Hackers vallen de mens aan omdat die vaak de zwakste schakel is.

2. De 4 Grote "Rode Vlaggen" (Signalen)

De Google Phishing Quiz leert ons dat we niet op ons gevoel mogen afgaan, maar actief moeten controleren. De 4 hoofdcategorieën van "rode vlaggen" zijn:

1. Controleer de LINK (URL) Dit is de meest voorkomende valstrik. Je moet altijd controleren waar een link écht naartoe gaat, door er met je muis over te zweven (hoveren).

- Let op een **"nep-URL"**.
- Controleer of de **domeinnamen** wel overeenkomen (gaat de link echt naar bol.com of naar bol.com.login-nu.xyz?).
- Hackers **verbergen** de echte link (bv. met 'tinyurl') om je naar een nep-inlogpagina te sturen.

2. Controleer de AFZENDER Kijk altijd kritisch naar wie de e-mail of sms stuurt. De naam kan echt lijken, maar het adres erachter is dat vaak niet.

- Let op pogingen om het **echte e-mailadres te verbergen**.
- Een SMS-bericht (bv. van Netflix) dat van een **e-mailadres** komt, is een grote rode vlag.

3. Let op de BOODSCHAP (De psychologische trucs) Hackers proberen je te manipuleren. Ze gebruiken psychologische trucs om je snel en onvoorzichtig te laten handelen.

- Ze gebruiken een **gevoel van urgentie** (haast), zodat je niet goed oplet.
- Let op een **"verdachte aanbieding"** of een aanbieding die **"te mooi was om waar te zijn"**.

4. Wees waakzaam met wat ze VRAGEN Phishing heeft vaak als doel om je iets te laten doen: een code geven of een gevaarlijk bestand openen.

- Deel **nooit een code voor tweestapsverificatie** als je niet zelf net op dat moment aan het inloggen was.
- Wees voorzichtig met **hyperlinks en bijlagen** (zoals .zip of .exe).


4 hoofdcategorieën
Controleer de LINK (URL)
Controleer de AFZENDER
Let op de BOODSCHAP
(De psychologische trucs)
Wees waakzaam met wat ze VRAGEN

3. Phishing in de Praktijk

Bijvoorbeeld:

CEO-Fraude (Whaling) Dit is een specifieke en gevaarlijke vorm van phishing, gericht op bedrijven

- **Wat is het?** De hacker doet zich voor als de CEO (de 'grote baas') of een manager.
- **Scenario:** Je bent op stage en krijgt een mail van de 'baas': "Ik zit in een meeting en kan niet bellen. Betaal dringend factuur X van €5.000 naar deze nieuwe leverancier."
- **De Truc:** Ze gebruiken **urgentie** ("dringend") en **autoriteit** (de baas) om je te laten betalen.

De Oplossing in een Bedrijf: Rapporteren In elk bedrijf is er een duidelijke procedure:

1. **Twijfel? Klik NIET.** De gouden regel is: "Wees sceptisch".
2. **Verifieer via een ander kanaal.** Kreeg je een raar verzoek van de baas via e-mail? **Bel** hem op zijn gekende gsm-nummer (NIET het nummer in de mail) om te checken of het echt is.
3. **Rapporteer.** Bedrijven hebben hiervoor professionele tools. Je gebruikt de **"Phish Alert"-knop** in Outlook . Dit verwijdert niet alleen de mail bij jou, maar waarschuwt ook onmiddellijk de IT-afdeling, zodat zij het bedrijf kunnen beschermen.

4. Wat als je toch klikt? (Malware)

Als je per ongeluk op een link in een phishingmail klikt, kunnen hackers **Malware** (Malicious Software) op je computer installeren. De gevaarlijkste vorm voor bedrijven is **Ransomware** (Gijzelsoftware).

- **Wat doet het?** Het versleutelt (encrypt) al je bestanden. Je computer wordt onbruikbaar en je ziet enkel een scherm met een klok die aftelt.
- **Het gevolg:** De hacker eist losgeld (ransom) om je bestanden terug te geven.
- **Impact op B&O:** Voor een bedrijf is dit een ramp. De productie stopt, winkels kunnen niet verkopen en de reputatie is kapot.

5. Je Verdedigingsmuur: De 3 Pijlers

Hoe bescherm je jezelf en een bedrijf hiertegen? Door een "muur" te bouwen met 3 lagen:

1. MFA (Multi-Factor Authentication)

- **De Regel:** Je wachtwoord alleen is niet genoeg (want dat kan gestolen zijn).
- **De Oplossing:** Gebruik Tweestapsverificatie (2FA/MFA).
    - Stap 1: Iets wat je **WEET** (je wachtwoord).
    - Stap 2: Iets wat je **HEBT** (je smartphone, een code, je vingerafdruk).
- Zet dit overal aan waar het kan (Instagram, Smartschool, Bank)!

2. Updates (De Kasteelmuur)

- Updates zijn geen pesten. Software is als een **kasteelmuur**.
- Na verloop van tijd ontstaan er barstjes (beveiligingslekken) in de muur. Hackers zoeken die barstjes om binnen te kruipen.
- Een **Update** is de metselaar die de barstjes dichtmaakt vóór de vijand ze vindt. Klik dus altijd op "Nu updaten".

3. Back-ups (De Levensverzekering)

- Als je toch slachtoffer wordt van Ransomware, is er maar één redding: een **Back-up** (reservekopie).
- Als je een goede back-up hebt, hoef je het losgeld niet te betalen. Je wist de computer en zet de kopie terug.
- **De 3-2-1 Regel:**
    - Zorg voor **3** kopieën van je bestanden.
    - Op **2** verschillende soorten media (bv. op je laptop én in de cloud).
    - Bewaar **1** kopie op een andere locatie (of offline), voor als het gebouw afbrandt of de cloud gehackt wordt.