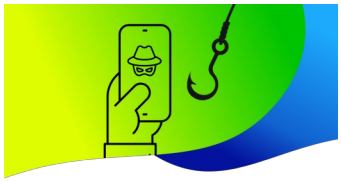
Jaargang 3 (2022) nummer 04

Wat is vishing?



Gebeld worden met de vraag geld over te maken. Het gebeurt en criminelen hebben er succes mee.
Ze pakken dit zogenaamde 'vishing' dan ook steeds slimmer aan.
Zo melde **de NOS dat Engelstalige neptelefoontjes** in minder dan een jaar tijd wel minimaal 1,7 miljoen euro aan schade hebben veroorzaakt.

Een samenstelling van *voice* en *phishing*
Phishing kennen de meeste mensen wel: je krijgt een e-mail met een link, zogenaamd van uw bank of energiebedrijf. Als je erop klikt kom je in een nepomgeving waar je kan inloggen en zo worden je gegevens gestolen. Phishing kan ook via de telefoon gebeuren. We noemen dit *vishing*. Een samenstelling van *voice* en *phishing*.

Lees ook: zo herken je een phishing e-mail
Hoe werkt vishing?
Stel, je wordt gebeld door je bank. Er is een verdachte inlogpoging geweest op je rekening en nu is het noodzakelijk dat je jouw geld veiligstelt door het op een andere rekening te zetten, een zogenaamde 'kluisrekening'. De boodschap wordt met veel urgentie gebracht en de bankmedewerker helpt vriendelijk mee om de overboeking meteen uit te voeren. Hop: spaargeld weg.

Het overkomt mensen werkelijk. Dat het lukt is dankzij de gewiekste psychologische trucjes van de cyberoplichters. Maar ook dankzij *spoofing*: waarmee een willekeurige beller zich kan vermommen als – bijvoorbeeld - het nummer van de bank. Deze oplichters doen zich niet alleen voor als bank, maar ook bijvoorbeeld als de Belastingdienst (vordering, onmiddellijk te betalen) of computerbedrijf (er is iets mis en uw inloggegevens zijn nodig).

Lees ook: dit is spoofing
Wat doet je ertegen?
Je kan je moeilijk wapenen tegen vishing. Deepfake stemmen zijn er vrijwel niet uit te filteren en spoofing is ook niet technisch te signaleren (al heeft Apple naar verluid een patentaanvraag gedaan op een techniek die spoofing herkent). Vooral goed opletten is dus het advies.

Lees ook: wat is deepfake?
Waar let je op?
Om te beginnen: wanneer 'je bank' belt en vraagt geld over te maken, moeten alle alarmbellen gaan rinkelen. Een bank zal dit nooit telefonisch aan je vragen. Het is dus belangrijk om niet mee te gaan in het gevoel van stress dat de beller wil veroorzaken. Vraag rustig om telefoonnummer, naam en achternaam, en zeg dat je terugbelt.
Bel vervolgens naar het echte nummer van je bank. Dubbelcheck het telefoonnummer via de website.

Trap ook niet in dreigende taal wanneer iemand je belt namens de Belastingdienst bijvoorbeeld over een openstaande betaling die meteen voldaan moet worden. Woorden als beslaglegging en invorderingskosten zorgen bij veel mensen op zijn minst voor lichte paniek, maar trap er niet in. Maak geen geld over maar bel eventueel zelf de Belastingdienst als je denkt dat er echt iets aan de hand is.
Ben je benaderd door kwaadwillende? Breng dan ook altijd de organisatie waarvoor ze zich voordeden op de hoogte. Zo kunnen ze ook andere mensen waarschuwen.