Phishing

Fraude via ' *Phishing* ' is al zo oud als het internet. Maar wat is het eigenlijk? Wij vertellen je hoe het werkt, welke verschillende methodes er gebruikt worden, en hoe je phishing kan herkennen. Een gewaarschuwd M/V/X is er twee waard!

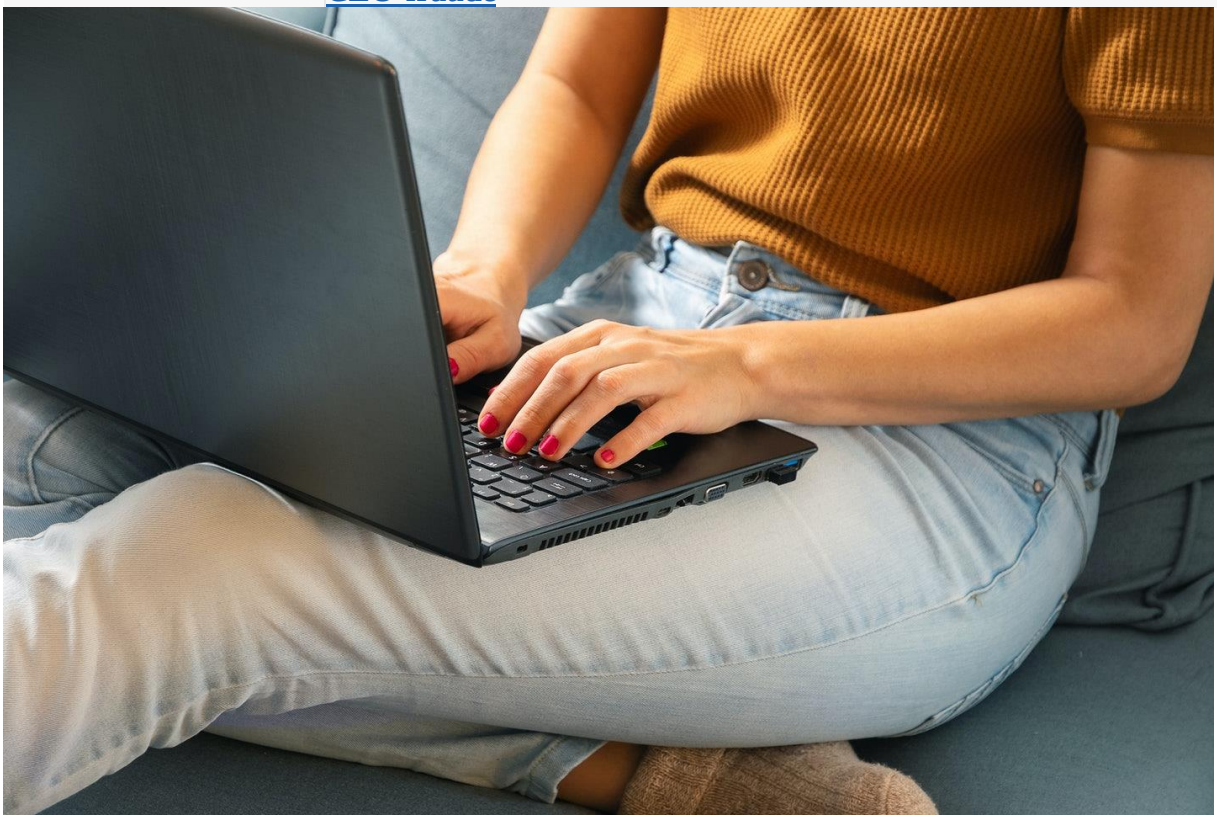
De verschillende soorten phishing

De term 'Phishing' heeft betrekking op het misleiden van mensen via het internet, om hen zo aan te zetten persoonlijke informatie te onthullen, zoals wachtwoorden en kredietkaartnummers. Maar ook om hen een *malware* te laten installeren. Dat kan een computervirus zijn dat alle bestanden op de computer besmet of versleutelt (ransomware), of spyware die bedrijfsgeheimen steelt.

Meestal denk je bij phishing aan frauduleuze e-mails, maar phishing kan ook via andere kanalen uitgevoerd worden. We onderscheiden:

	Voorbeeld
Vishing (voice + phishing): phishing via telefoon	de zogenaamde telefoontjes van Microsoft, waarin je de vraag krijgt om jouw wachtwoord te geven, of waarbij jij allerlei handelingen moet uitvoeren o.a. bestand downloaden.

Smishing: (sms + phishing): phishing via sms	je krijgt een melding via SMS met daarin een link die je naar een frauduleuze site vo
Spear Phishing: specifiek naar een groep personen gericht	je krijgt een mail die alle kenmerken vertoont van een mail van je bank, maar niet va je bank afkomstig is. Je klikt op de link, en belandt op een perfect nagemaakte webs van je bank. In goed vertrouwen log je in, en zo bemachtigt de crimineel jouw gegevens.
Whaling: nog meer doelgerichte spear phishing	een fraudeur viseert de CEO, CFO, COO van een bedrijf of mensen met een hoge positie. Hij gebruikt informatie die hij op social media vindt om het slachtoffer het gevoel te geven dat de mail echt is ('social engineering'). Doel: bedrijfsspionage, financiële fraude (valse overschrijving laten uitvoeren), enz. Lees meer: "**Pas op voo CEO-fraude**"



De verschillende methodes gebruikt bij phishing

E-mail spoofing

Hoe? De aanvaller gebruikt een vals e-mailadres. Jij krijgt een mail die afkomstig lijkt van een persoon die je kent of een bedrijf waar je klant bent. Vaak zal de oplichter een bestaand formulier van dat bedrijf perfect nabootsen, zoals een ontvangstbewijs voor een transactie.
Waarom? De fraudeur vraagt jou om op een link te klikken, in te loggen en bepaalde actie te ondernemen, zoals bestanden te delen.
Hoe herken je de aanval? Jouw naam staat niet vermeld in het 'Aan' vakje, of staat er tussen een hele rij andere mensen die jij niet kent; of je bent

geen klant bij dit bepaald bedrijf, althans niet met het mailadres waarnaar de mail verzonden werd.

URL Phishing

Hoe? De fraudeur camoufleert een webadres of URL in een mail of ander bericht zodanig, dat dit op een betrouwbaar adres lijkt. Hij hanteert daarbij deze technieken:

- de link is verborgen onder een knop 'Klik hier' of 'Abonneer je nu'
- de link is verkort met een link-verkorter zoals t.co/xz92drTT92
- de link is een foutieve spelling van een bekend bedrijf, bijvoorbeeld citiibank.com in plaats van citibank.com
- de link is een homografische variant, bijvoorbeeld arnazon.com in plaats van amazon.com, of Faceb00k.com in plaats van Facebook.com

De aanvaller heeft vooraf deze foutieve domeinnamen geregistreerd. Klik je de link aan in een mail of andere boodschap, dan word je naar die nagemaakte website gevoerd.

Waarom? Jouw gegevens bemachtigen, malware installeren, enz.

Hoe herken je het? Beweeg de cursor over de link. De volledige link zal op je scherm verschijnen. Bij je mobiele toestel lang-druk je op de link, en de volledige link zal in een pop-up verschijnen. Je kan ook rechts-klikken op de link, en naar je notitieblok kopiëren.

Subdomein aanval

Hoe? Een weblink bevat de naam van een gekend bedrijf, wat jouw vertrouwen wekt. Maar als je het adres nader inspecteert, zal je bemerken dat de weblink helemaal niet naar de domeinnaam verwijst van dat gekende bedrijf - het is een subdomein van een domein, in handen van de aanvaller!
Hoe herken je het? Bestudeer altijd nauwkeurig een webadres. Begin van rechts naar links - de woordcombinatie VOOR de / is de domeinextensie, met links daarvan de domeinnaam. Alles wat zich daarvoor bevindt, is een subdomein.
Voorbeeld: *https://inlog.dnsbelgium.be.bijdeneusgenomen.be/jouwaccount*. Hierbij is "bijdeneusgenomen.be" de domeinnaam en "dnsbelgium.be" een subdomein van de domeinnaam.

Phishing via pop-up vensters

Hoe? Je bezoekt een gewone website, en plots verschijnt er een pop-up venster. Dat vraagt je om in te loggen op bijvoorbeeld de website van je provider. Dit is 'in-session phishing'. Bij Malvertising wordt van deze techniek gebruik gemaakt. Lees meer: '**Fraude via malvertising**'
Ons advies: deze pop-ups kunnen heel hardnekkig zijn; zij verdwijnen vaak niet door op de Escape-toets te drukken of het kruisje in de rechter

bovenhoek. Sluit het tabblad en surf opnieuw naar de website. Sluit desnoods je *browser* .

Phishing via de zoekmachines

Hoe? De aanvaller bouwt een perfecte kopie van de website van een bekend bedrijf na. Hij plaatst bij een zoekmachine zoals Google een advertentie, met de naam van dat bedrijf als trefwoord. Tik jij bij die zoekmachine de naam van het bedrijf in, dan zal de website van de aanvaller tussen de gesponsorde links staan, bovenaan de zoekresultaten.
Hoe voorkom je het? Mijd de advertenties bovenaan de zoekresultaten, herkenbaar aan de 'ad' vermelding naast de link. Wees vooral wantrouwig wanneer je gelokt wordt met extra kortingen en superaanbiedingen. Ken je het webadres van het bedrijf, tik het gewoon in de adresbalk in.

Phishing door filters te omzeilen

Hoe? De meeste filters in je mailprogramma en van je antivirus zullen je waarschuwen wanneer je een verdachte link aanklikt om te openen in je browser. De aanvaller maakt daarom de link niet-aanklikbaar en geeft instructie om de link met copy/paste naar je browser te kopiëren. Zo omzeilt de aanvaller de filters.
Hoe voorkom je het? Vertrouw dergelijke mails niet! Ga niet in op het verzoek om de link te kopiëren.

Het anti-phishing harnas dat je zo goed mogelijk beschermt

Een gezonde dosis wantrouwen kan al heel wat narigheid voorkomen. Pas deze regels toe:

- Word je opgebeld door een bedrijf dat je vraagt handelingen uit te voeren aan de computer, ga hier niet op in. Vraag de naam en het telefoonnummer van de persoon, en zeg dat je zelf zal terugbellen. Ondertussen kan je achterhalen of het telefoonnummer wel degelijk tot jouw bank, of tot het genoemde bedrijf behoort.
- Let op met e-mails, vooral wanneer zij niet rechtstreeks aan jou gericht zijn, en vol spelfouten staan.
- Ontleed altijd de links in e-mails. Kopieer de link naar je notepad, als gewone tekst.
- Maak gebruik van een wachtwoord-manager
- Activeer two-factor authenticatie bij elke website of webdienst die dit aanbiedt
- Gebruik zoveel mogelijk beveiligde websites, herkenbaar aan "https" in het webadres en het gesloten slot.
- Zorg ervoor dat je antivirus altijd up-to-date is
- Installeer meteen de nieuwste updates van je besturingssysteem, je mailprogramma, browser, en alle software die je gebruikt.
- Het **Centrum voor Cyberveiligheid in België en de Cyber Security Coalition** stellen materiaal ter beschikking om gebruikers te sensibiliseren voor de gevaren van phishing. **Download de cyber security kit** en verspreid de boodschap onder je collega's, je gebruikers, je leerlingen.
- Merk je een poging tot phishing op? Of ben je slachtoffer van een phishing-aanval? Dien altijd klacht in bij de politie - zo voorkom je dat ook anderen slachtoffer worden. **Hier** vind je de instructies.

Hou het veilig!