HOE KAN MEN PHISHING OF SMISHING VOORKOMEN?

written by Yannick Lauwers | mei 2, 2023

In onze vorige bijdrage[1] kon u al lezen dat phishing in 2020 en 2021 een echte plaag vormde. Deze vorm van digitale inbraak lijkt in 2023 nog steeds bijzonder populair te zijn. Phishers blijken zeer vindingrijk en bedenken geregeld nieuwe kunstgrepen om mensen geld of gegevens afhandig te maken.

Phishing is een vorm van cybercriminaliteit waarbij het potentiële slachtoffer wordt benaderd via e-mail, sms, sociale media of telefoon. De oplichter doet zich daarbij voor als iemand anders in een poging toegang te krijgen tot de vertrouwelijke gegevens van slachtoffers.

Smishing vormt de sms-variant van phishing. Zo kan het zijn dat een verzonden sms een link bevat die de browser op de telefoon naar een website stuurt die kwaadaardige software (malware) installeert. Door op deze link te klikken, kunnen bankgegevens worden ontfutseld om zo iemands rekening te plunderen.

Deze oplichtingsmethodes zijn door de jaren heen ook steeds moeilijker te herkennen. Het onderscheid maken tussen valse e-mails en betrouwbare berichten, lijkt haast een onmogelijke opdracht geworden. Desondanks willen we u met een aantal tips wapenen om het risico op phishing of shmishing tot een minimum te beperken.

Twijfel je of een bericht verdacht is? Beantwoord dan kort voor jezelf deze vragen:[2]

- Is het bericht onverwacht?
- Is het bericht dringend geformuleerd?
- Ken je de afzender?
- Vind je de vraag die wordt gesteld vreemd?
- Naar waar leidt de link waar je moet op klikken? (*Tip: beweeg over de link (maar door deze nooit open!) en kijk waar deze u naartoe stuurt. Een verdachte link doet u best niet open.)*
- Word je persoonlijk aangesproken?
- Bevat het bericht veel taalfouten?
- Zit het bericht in je Spam?

- Probeert iemand je nieuwsgierig te maken?

Besluit

Phishing of smishing is een fenomeen dat elk jaar op grote schaal toeneemt. Met de verdere digitalisering van de samenleving lijkt het probleem zich op de korte termijn dan ook niet zomaar op te lossen. Het beste advies dat we u als lezer kunnen meegeven is dan ook om steeds aandachtig te zijn voor 'vreemde' berichten die u binnenkrijgt via e-mail of sms. Een bericht dat te mooi is om waar te zijn, zal dit meestal ook zijn.

Zit er een reukje aan een bepaalde transactie die je hebt verricht? Contacteer zo snel mogelijk Card Stop om je kaart te laten blokkeren. Dit kan op het nummer 070 344 344. Weet dat Card Stop nooit mensen zal opbellen. Geeft iemand zich aan de telefoon uit als een medewerker van Card Stop, dan is dit 100% een oplichter.

Krijgt u een verdacht bericht via mail of per sms, aarzel dan zeker niet om dit bericht door te sturen per mail naar verdacht@safeonweb.be. Zij controleren de links en bijlages van deze doorgestuurde berichten waarbij ze in staat zijn om verdachte links te laten blokkeren. Op die manier zijn minder oplettende internetgebruikers die op de link geklikt hebben, ook beschermd. Door snel te ageren, verkleint de kans dat cybercriminelen slachtoffers maken. Een gewaarschuwd man is er twee waard.

Indien u na het lezen van dit artikel nog vragen hebt omtrent phishing, aarzel dan niet om ons te contacteren via joost.peeters@studio-legale.be of 03 216 70 70.

[1]https://www.studio-legale.be/phishing-het-nieuwe-inbreken-anno-2021/?lang=nl ; https://www.jubel.be/phishing-het-nieuwe-inbreken-anno-2021/

[2] https://www.safeonweb.be/nl/leer-valse-mails-herkennen