Hoe herken je Phishing?

Al in de 70-jaren kwam cybercrime voor. Vanaf 1996 ging men het Phishing noemen. Dan praten we al over een kleine 30 jaar geleden.
Doordat de computers tegenwoordig zo dicht gespijkerd zijn voor hackers neemt Phishing alleen maar toe.
Inmiddels zijn er meerdere vormen van Phishing zoals Phishing zelf, Spear Phishing, Walvis Phishing, Vishing, Smishing, Business email compromise, Clone Phishing, Catphishing, WhatsApp-fraude, randsomware, Ddos-aanvallen, identiteitsfraude, malware, virussen en nog veel meer.
Het is nu bijna een dagelijkse uitdaging voor een gemiddelde internet gebruiker om Phishing te ontdekken en af te stoppen.

Wat is phishing.
Phishing is waarbij criminelen via valse misleidende e-mails, telefoontjes of sms'jes proberen inloggegevens zoals wachtwoorden, bankgegevens, creditcardnummers met wachtwoorden, online inloggegevens voor sociale mediaprofielen en meer te stelen.
Het lijkt alsof ze van een betrouwbare bron komen, zoals een bank of een bekende dienst.
Het kan ook een e-mail zijn die lijkt alsof hij van een familielid, of een beroemd iemand af komt of van een grote organisatie, zoals deurwaarde bureaus, PayPal, Amazon, Microsoft, ziggo, kpn, banken, overheidsinstantie en zelfs van de HCC.
De berichten lijken echt en dringend. Dit om angst te zaaien, waarbij ze de slachtoffers verleiden om op links te klikken, malware te downloaden of worden omgeleid naar valse websites om inloggegevens, financiële gegevens af te geven of om geld over te maken.
De niets vermoedende slachtoffer is hierdoor kwetsbaar voor identiteitsdiefstal en financieel verlies.
Phishing is bijzonder effectief omdat het misbruik maakt van de menselijke psychologie in plaats van geavanceerde technische tactieken. Vaak vermomd als dringende mededelingen van gezaghebbende figuren, maken phishing-oplichtingen gebruik van het vertrouwen en de angst van mensen.

Hoe herken je Phishing.
1. Let op onregelmatigheden of eigenaardigheden in de e-mail. Door waakzaam te zijn.
2. Gebruik de "geurtest" om te bepalen of er iets niet klopt volgens jou.
3. Vertrouw op uw instincten, maar blijf uit de buurt van angst, want phishing scams maken vaak gebruik van angst om het oordeel van jou te beïnvloeden.
4. Bij twijfel neem zelf contact met voor jou bekende wegen met de bewuste instantie/persoon (bank, bedrijf of belastingdienst) en vraag om bevestiging dat de informatie wel of niet klopt.
5. De e-mail kan een aanbod bevatten dat te mooi is om waar te zijn. Het kan beweren dat je de hoofdprijs hebt gewonnen, een extravagant cadeau, of andere onwaarschijnlijke beloningen.
6. De afzender van een mail of sms-bericht is herkenbaar, maar niet iemand met wie je normaal gesproken contact heb. Wees voorzichtig als je de naam van de afzender zelf herkent of als het niet iemand is met wie je regelmatig communiceert of vooral als de inhoud van de e-mail niets te maken heeft met je gebruikelijke taken. Wees ook op je hoede als je op c.c. staat met onbekende personen of collega's uit niet-gerelateerde afdelingen.
7. De boodschap boezemt angst in. Wees voorzichtig als de e-mail geladen of alarmerende taal gebruikt om een gevoel van urgentie op te wekken, waarbij u wordt aangespoord om te klikken en "onmiddellijk te handelen" om te voorkomen dat de account wordt beëindigd. Onthoud dat legitieme organisaties niet om persoonlijke informatie vragen via e-mail.
8. Het bericht bevat onverwachte of vreemde bijlagen. Deze bijlagen kunnen malware, ransomware of andere online dreigingen bevatten.
9. Het bericht bevat links die twijfelachtig lijken. Zelfs als de bovenstaande indicatoren geen argwaan wekken, vertrouw ingebedde hyperlinks nooit blindelings. Beweeg je cursor over de link om de werkelijke URL te onthullen. Let vooral op subtiele spelfouten in een ogenschijnlijk bekende URL van een website, want dat is een waarschuwingssignaal voor bedrog. Het is altijd veiliger om de URL handmatig in je browser in te voeren in plaats van op de ingesloten link te klikken. Verder waar je op kan letten is onbekende afzender e-mailadressen, algemene begroetingen, spel- en grammaticafouten en misleidende URL's.
10. Controleer of de URL van de pagina begint met "HTTPS" in plaats van alleen "HTTP". De "S" staat voor "secure". Het is geen garantie dat een site legitiem is, maar de meeste legitieme

sites gebruiken HTTPS omdat het veiliger is. HTTP-sites, zelfs legitieme, zijn kwetsbaar voor hackers

11. Kijk uit naar het digitale certificaat van een website. Om die bescherming te versterken, als je een e-mail krijgt van een bron waar je niet zeker van ben, navigeer dan handmatig naar de gegeven link door het legitieme websiteadres in te voeren in uw browser. Beweeg de muis over de link om te zien of het een legitieme link is. Als je vermoedt dat een e-mail niet legitiem is, neem dan een naam of een tekst uit het bericht en voer die in een zoekmachine in om te zien of er bekende phishing-aanvallen bestaan waarbij dezelfde methoden worden gebruikt.

Alex Hol