WWW.MINDYOURSTEP.INFO

Phishing

hoe blijf je zo alert mogelijk?

De vraag

Phishing, ofwel het 'vissen' naar informatie, is op dit moment één van de meest gebruikte vormen van digitale oplichting. Het is een methode waarbij je via e-mail verleid wordt om gevoelige informatie, zoals wachtwoorden, beveiligingscodes en bankgegevens, te verstrekken. Ook wordt het gebruikt om malware op apparaten en bedrijfssystemen binnen te smokkelen. Kortom, phishing kan vele vormen aannemen. En er is nog meer..
Er is ook nog iets wat spear-phishing genoemd wordt. Hierbij gaan aanvallers nóg een stapje verder en is de aanval op jou als persoon gericht. In dit geval sturen aanvallers een e-mail die afkomstig lijkt te zijn van een collega, je leidinggevende of zelfs de ICT-afdeling. Door middel van informatie die de aanvallers over jou weten, kunnen zij het bericht vertrouwelijk over laten komen. Op die manier proberen deze aanvallers naar nog meer informatie te 'vissen' en kunnen zij jou bijvoorbeeld een schadelijk bestand laten downloaden of zelfs geld laten overmaken. Phishing kan dus heel ver gaan. Hoe kun je jezelf hier tegen beschermen en belangrijker; hoe kun je een phishing aanval herkennen?

De uitdaging

Zelfs als je heel oplettend bent, is het soms moeilijk om een phishing e-mail te herkennen. Dat komt omdat vaak bestaande bedrijven worden gebruikt als afzender. Misschien heb je weleens een phishing e-mail ontvangen? Bijvoorbeeld een e-mail in de huisstijl van je bank, waarin gevraagd wordt om bepaalde zaken over jouw rekening te bevestigen? De berichten zijn dan zo overtuigend dat je er gemakkelijk intrapt als je niet alert genoeg bent. Of een nepfactuur waarin gevraagd wordt om een bijlage te openen om je aankoop te bevestigen? Of misschien ben je weleens via advertenties en links naar een aanmeldpagina op een website doorverwezen. De e-mails en websites waarnaar gelinkt wordt, zijn niet meer van echt te onderscheiden. Daarnaast worden internetcriminelen die deze methode toepassen steeds doordachter.

De oplossing

De oplossing is eigenlijk even simpel als complex; alertheid. De volgende tips kunnen je hierbij helpen:

- Een onpersoonlijke aanhef. Een phishing e-mail is vaak onpersoonlijk, de aanhef luidt bijvoorbeeld 'Beste klant'. Maar let op: ook een gepersonaliseerde e-mail kan nog steeds nep zijn!
- Slecht taalgebruik en taalfouten. Je kunt phishing e-mails vaak herkennen aan slecht taalgebruik en spelfouten in het bericht. Andere aandachtspunten zijn: het ontbreken van, of teveel spaties/punten en hoofdlettergebruik.
- Links met een vreemde tekst. Controleer altijd de links die in e-mail berichten staan. Het kan zijn dat deze verwijzen naar een hele andere website. Wanneer de e-mail een phishing link bevat staat er vaak een reeks cijfers (het IP-adres) aan het begin van de link.
- Bijlagen in de vorm van ZIP-bestanden. De bijlagen met ZIP-bestanden van phishing e-mails bevatten vaak virussen. Open deze dus nooit wanneer je de herkomst van het bericht niet vertrouwt.
- Een onbekend of onjuist e-mailadres. Open geen e-mails van personen die je niet kent of e-mails die je niet vertrouwt. Heb je per ongeluk toch een bericht geopend dat je niet vertrouwt? Klik dan nooit op de links in het bericht en open ook geen bijlagen. Zo voorkom je dat eventuele virussen verspreid worden.
- Check de afzender van het bericht. Bedrijven of banken vragen nooit om persoonlijke gegevens of inloggegevens via e-mail. Dus geef je gegevens nooit prijs.

Tot slot.. gebruik een goede virusbescherming of anti-spam software om de kans op phishing te verkleinen. Twijfel je over de authenticiteit van een e-mail? Neem dan altijd contact op met de betreffende instantie en zoek het telefoonnummer dan op via de officiële website.

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak.
Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.