

Links in e-mail- en online berichten (via sms of websites) zijn vaak de manier waarop criminelen een computer binnendringen. Ze proberen gebruikers te verleiden om op een link te klikken of een bijlage te openen die hun computer infecteert met virussen of malware.

Phishing e-mails kunnen heel echt lijken; alertheid is altijd geboden! Volg daarom onderstaande tips.

1 > GOOI WEG BIJ TWIJFEL

Verwacht je een bericht niet of ziet het er verdacht uit, controleer eerst het domein (wat achter @ staat). Zelfs als de bron bekend is, informeer bij de IT-helpdesk of meer mensen het bericht hebben gekregen. Blijft er twijfel? Meld het bericht (intern) als phishing, verwijder of markeer als 'ongewenst'. Neem persoonlijk of telefonisch contact op met de afzender om zeker te zijn dat de e-mail niet legitiem is.

2 > DENK NA VOORDAT U HANDELT

Wees op uw hoede voor communicatie die u vraagt om onmiddellijk te handelen, iets aanbiedt dat te mooi klinkt om waar te zijn én waarin om persoonlijke en/of bedrijfsinformatie wordt gevraagd.

3 > MAAK WACHTWOORDEN LANG EN STERK

Gebruik minstens 16 karakters, indien mogelijk in combinatie met multifactor authenticatie (mfa). Combineer hoofdletters en kleine letters met cijfers en symbolen. Kies bij voorkeur drie willekeurige woorden, liefst met spaties. Overweeg of bespreek de mogelijkheid om een wachtwoordmanager te (gaan) gebruiken die het bedrijf beschikbaar stelt.

4 > PAS OP VOOR HYPERLINKS

U kunt een gehyperlinkt woord of URL controleren door de muis op het woord te plaatsen om het volledige adres weer te geven. Bij voorkeur wordt het klikken op hyperlinks in e-mails vermeden; typ de URL rechtstreeks in de adresbalk.

5 > MAAK GEBRUIK VAN BETROUWBARE BRONNEN

<https://haveibeenpwned.com/> - Hier kun je jouw mailadres invullen om te kijken of deze ooit gelekt is. Samen met het wachtwoord, om vervolgens je wachtwoord te veranderen indien blijkt dat deze gelekt is.

<https://checkjelinkje.nl/> - Hier kun je eenvoudig controleren of een link in een mail wel of niet veilig is.



Meer informatie over dit onderwerp deelt Cyber Weerbaarheidscentrum Brainport met haar participanten. Ook lid worden van deze stichting zonder winstoogmerk? Bezoek www.cwbrainport.nl of mail naar info@cwbrainport.nl.

Met dank aan