****

**Copy**

Laat je niet interneppen

Check de afzender en bij twijfel: klik weg!

Zo’n 2,2 miljoen mensen kregen vorig jaar te maken met online criminaliteit. Door de slimme manieren van online misleiding kan iedereen in de val trappen. Interneppers ofwel internetcriminelen doen zich voor als iemand anders om jouw gegevens te stelen of om je op te lichten via mail, sms of WhatsApp. Het bericht of de mail komt op het eerste gezicht van iemand die je vertrouwt. Zoals een vriend, een medewerker van een winkel met een mooie aanbieding of zelfs van je bank. Als ze voor je staan trap je er misschien niet zo snel in, maar online is dat een stuk lastiger. De beste manier om hiermee om te gaan? De afzender checken en als je het niet vertrouwt of twijfelt: wegklikken.

De Internepper

* De internepper doet er alles aan om zo betrouwbaar mogelijk over te komen en doet zich daarom voor als een bekende of een instantie.
* Het lijkt alsof de internepper veel van je weet, bijvoorbeeld je naam, dat je op vakantie was of dat je een kamer zoekt.
* De internepper verzamelt vaak eerst informatie over je via jouw social media

Social Engineering

Een internepper doet aan Social Engineering. ’Social Engineering' is een term voor wisselende trucjes waarmee mensen online worden bedrogen. Door zich voor te doen als iemand anders en door handig in te spelen op persoonlijke situaties, krijgen internetcriminelen het voor elkaar om je op het verkeerde been te zetten. Engineering betekent eigenlijk ‘iets bouwen. Bij social engineering bouwen criminelen als het ware een omgeving of situatie waarin ze jou zo manipuleren dat je gevoelige informatie deelt of geld betaalt.

Ze doen dit door gebruik te maken van eigenschappen die we allemaal hebben:

* Nieuwsgierigheid naar een mooie aanbieding
* Angst voor een financiële noodsituatie
* Behulpzaamheid voor een kleindochter in nood

Een aantal voorbeelden

1. Nepmails

Nepmails namens je bank of zelfs van de Rijksoverheid. Hierin kan gevraagd worden om op een link te klikken en je (bedrijfs)gegevens te delen. Dan is er sprake van ‘phishing’.

2. Malware

De link kan ook malware bevatten, een programma waarmee een crimineel ongevraagd toegang krijgt tot je computer of apparaat. Hierdoor kunnen ze nog meer persoonlijke gegevens stelen, denk aan je identiteitskaart of paspoort, of je computer blokkeren in ruil voor geld (ransomware).

3. Hulpvraagfraude

Ook kun je een appje of berichtje krijgen van een zogenaamd familielid die in (geld)nood zit. Vaak wordt hier gevraagd om zo snel mogelijk actie te ondernemen

Hoe herken je misleidende berichten?

1. Je krijgt geen bedenktijd.
* Als je aarzelt, probeert de internepper je twijfels meteen weg te nemen.
* De internepper valt je constant lastig door berichtjes te sturen.
* De internepper doet aardig, behulpzaam en raakt niet geïrriteerd.
* Er blijft benadrukt worden dat je direct moet handelen.
1. Het bericht heeft een dwingende toon.
* De zogenaamde ‘bekende’ of ‘instantie’ verwacht dat je iets betaalt.
* Er wordt verwacht dat je geld overmaakt.
* Je wordt gevraagd om op een link te klikken.
* Je wordt aangespoord om iets te downloaden.
1. De situatie escaleert
* Er wordt verteld dat er iets ergs gebeurd is.
* Je krijgt een aanbieding die te mooi is om waar te zijn.
* Je loopt gevaar geld te verliezen.
* De internepper vraagt dringend om jouw hulp.

Wat kan je zelf doen? Check de afzender en bij twijfel: klik weg!

1. Check de afzender

* Controleer het e-mailadres.
* Je herkent een vals e-mailadres door vreemde tekens of een naam die afwijkt van een bekend e-mailadres. Of het is een heel vreemd en ongeloofwaardig e-mailadres.
* Probeer via een bij jou bekend telefoonnummer of e-mailadres contact op te nemen met de afzender.
* Bij twijfel: klik weg!

2. Check de link

Als je een link van een website krijgt die je niet vertrouwt, nooit direct klikken.

* Als je de afzender niet vertrouwt, klik dan niet op een link.
* Ben je toch nieuwsgierig? Check dan de link via ScamCheck of checkjelinkje.nl.
* Let erop dat je de link opeen veilige manier kopieert (niet klikken dus!)
* Bij twijfel: klik weg!

3. Bescherm je zelf

* Let altijd goed op welke informatie je online deelt en met wie. Voor je social media-accounts kun je dit aanpassen bij de privacy-instellingen.
* Zorg ervoor dat je je gegevens goed beschermt. Deel je wachtwoord niet met anderen en probeer tweestapsverificatie (2FA) te gebruiken om je accounts nog beter te beveiligen.
* Bij twijfel: klik weg!

**Campagne**‘Laat je niet interneppen’ is een campagne die mensen helpt om online misleiding te herkennen én te voorkomen. De meerjarige campagne is een initiatief van het Ministerie van Justitie en Veiligheid en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en roept mensen op om goed de afzender van online berichten te checken en bij twijfel weg te klikken of swipen. De campagne is gericht op een breed publiek.