BETER BEGRIJPEN IS BETER BESCHERMEN

Inzicht in de trucs van cybercriminelen maakt dat u er minder snel slachtoffer van wordt!

De methodiek achter veel oplichting heet social engeneering. Social engineering gaat over trucs om een beoogd slachtoffer te laten meewerken aan de bedoelingen van de oplichter. Deze folder is gemaakt om deze trucs die criminelen gebruiken aan u uit te leggen. Zo gaat u sneller herkennen of u met een oplichter te maken heeft en kan u voorkomen dat u slachtoffer wordt.

Weet u niet goed hoe u uzelf moet beschermen tegen cybercriminaliteit, maar maakt u zich wel zorgen? Lees dan de tips in deze folder. Het is niet zo ingewikkeld en het maakt een groot verschil.

De methodiek achter veel cybercriminaliteit

Criminelen maken vaak gebruik van uw goedheid , uw hulpvaardigheid en uw wens om uit de problemen te blijven. Zo gaat het in zijn werk: U ontvangt een mail, een telefoontje of een appbericht waarin er plotseling een probleem wordt ‘gemeldt’. Er is haast geboden want:
- er verloopt een betalingstermijn;
- uw geld loopt gevaar en moet veilig gesteld worden;
- er dreigt een account opgeheven te worden;
- er dreigt een boete of beslaglegging.

Voelt u de stress al? Opschieten, opschieten, want anders...
Dat is precies waar criminelen u willen hebben! U wilt snel helpen of snel van de problemen af zijn. In deze snelheid denkt niet zo goed meer na en doet al snel automatisch wat ze van u vragen. Met alle ellende van dien.

1. Lees hieronder hoe het werkt;
2. Leer het patroon herkennen;
3. Voorkom daarmee dat u slachtoffer wordt.

Voorbeeld 1: Vriend-in-noodfraude

Een vriend, familielid of andere bekende verstuurt een bericht dat hij (of zij) dringend financiële hulp nodig heeft. Hij schrijft dat hij een nieuwe telefoon heeft waarmee hij of zij nog niet kan internetbankieren. Deze ‘bekende’ vraagt je om snel geld over te maken. (Herkent u het patroon? Er is een probleem én er is haast.)

Achteraf blijkt het account van deze vriend gehackt te zijn. Of er is een nep-profiel van diegene aangemaakt waar zogenaamd een nieuw telefoonnummer bij hoort. Door slim gebruik te maken van alle informatie over u op internet lijkt het verhaal te kloppen, wat de criminelen u willen laten geloven. Wees dus alert op het patroon: er is een probleem en er is haast bij.
Vriend-in-nood-fraude komt op WhatsApp verreweg het meeste voor maar kan ook plaatsvinden via e-mail en SMS.

Kijk voor een duidelijk voorbeeld van zo’n appgesprek op fraudehelpdesk.nl/thema/zoon-ontfutselt-geld-via-whatsapp

Dit overkomt mij niet!

Nu denkt u misschien: ‘Dat overkomt mij niet.’
Uit onderzoek blijkt dat bijna iedereen dat denkt, en toch zijn dit de feiten:
• 15 % van de Nederlanders heeft digitale oplichting meegemaakt ;
• De gemiddelde schade loopt van 750 tot 2.500 euro;
• 49,5 % van seniore slachtoffers ondervindt emotionele en psychische problemen zoals angst voor de toekomst, gebrek aan zelfvertrouwen of groter gevoel van eenzaamheid
Lees meer over de emotionele gevolgen van fraude op: fraudehelpdesk.nl/thema/het-leed-dat-fraude-heet/
• Mensen van 55 jaar en ouder worden het meest slachtoffer van vriend-in-noodfraude.

Alle reden dus om uzelf goed te beschermen. Lees hoe ze te werk gaan en neem de tips die verderop staan goed in u op.

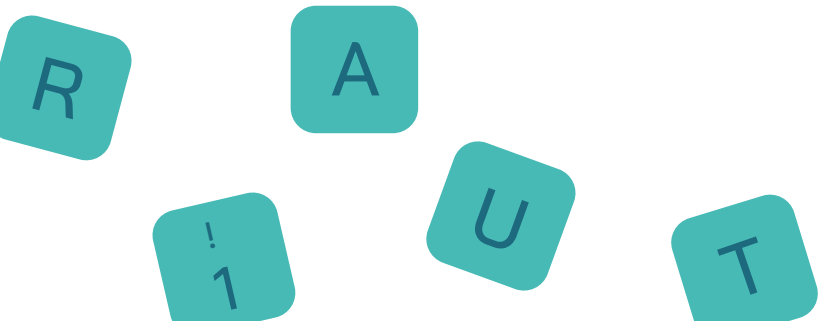
Voorbeeld 2: Dating fraude

Liefde is waar veel mensen naar verlangen. En om die te vinden maken we steeds meer gebruik van dating sites. Als u met een fraudeur te maken heeft gaat het kennismaken via de site vaak heel soepel en

de relatie neemt al snel een vlucht. Er wordt al snel veel kwetsbare informatie gedeeld. Als er echt een band is ontstaan komt het verzoek van de 'geliefde' om geld. Geld om een vliegticket te betalen of omdat er een plotseling probleem is. De zogenaamde geliefde geeft bijvoorbeeld aan dat hij een ongeluk heeft gehad en in het ziekenhuis ligt. Herken ook hier het patroon: er is een probleem (en u wilt maar al te graag helpen) en er is haast bij.
Een slachtoffer vertelt: 'Het leek wel of ik in een soort trance was geraakt. Helder nadenken kon ik niet meer. Ik werd blind meegezogen in de mooiste verhalen en beloftes.' Zij verloor meer dan €45.000,-.

Voorbeeld 3: Helpdeskfraude

U heeft het vast al vaker gehoord, maar een helpdesk belt nooit zelf op. Een helpdesk is er namelijk om uw telefoontjes te ontvangen. Zelf bellen met klanten kost teveel tijd. Toch woekert deze vorm van oplichting al jaren en wordt helaas nog veel toegepast door criminelen. Het patroon herkent u ondertussen waarschijnlijk wel. U wordt gebeld door een nep-helpdesk. Dat kan zijn van een groot computerbedrijf of van uw eigen bank bijvoorbeeld. Zoals te verwachten is er een acuut probleem met uw computer of met uw rekeningen. En inderdaad er is ook nu weer haast geboden. Nu het hier zo op papier staat lijkt het zo makkelijk te herkennen, maar de oplichters zijn geraffineerd en u moet sterk in uw schoenen staan om bestand te zijn tegen hun methoden. Laat u niet misleiden en wees gezond wantouwend!



Daarom hieronder de beste handvatten om online fraude te voorkomen.

Hoe bescherm ik mijzelf?

1. Herken het patroon
Tien minuten ervoor was er nog niks aan de hand en door een bericht dat u krijgt slaat acuut de stress toe. Dus herken het patroon: er wordt een acuut probleem gepresenteerd en er is haast om het op te lossen. U wordt aangespoord om betalingen te doen of wachtwoorden te delen. DOE HET NIET! Als u een nep-helpdesk aan de telefoon hebt en u voelt dat het foute boel is: hang gewoon op. Laat u niks aanpraten. In andere gevallen: stop het contact en ga door naar stap 2.

2. Vraag hulp
Vraag mensen in uw omgeving of ze even meedenken of meekijken wanneer u een bericht ontvangt waarbij u twijfelt over de echtheid. Ziet u een koopje op Marktplaats? Of twijfelt over een bericht van bijvoorbeeld de Belastingdienst. Is die wel echt? Wacht dan eerst op andermans oordeel voordat u verdere stappen zet.

3. Lees en praat erover
Ook als er nog geen directe aanleiding is, is het belangrijk om met vrienden en familie zo nu en dan over cybercriminaliteit te praten. Hoe herkent u het en wat spreekt u af voor een echt noodgeval? Zo kunt u echt van nep onderscheiden. Verder kunt u elkaar tips geven en alert houden om de nieuwe oplichtingsverhalen te herkennen.

Wat moet ik doen als ik toch slachtoffer word?

Mocht u toch slachtoffer worden van oplichting, schaam u dan niet! Het kan namelijk iedereen overkomen.

1. Praat erover, lucht uw hart
Laat vooral aan anderen weten dat u slachtoffer bent geworden. Informeer bijvoorbeeld uw familie of vrienden zodat jullie samen kunnen kijken welke stappen er gezet moeten worden. Voelt u zich dom of schuldig, dat is begrijpelijk, maar is echt niet nodig. U kunt ook uw verhaal delen bij slachtofferhulp. Blijf er in ieder geval niet in uw eentje mee rondlopen.

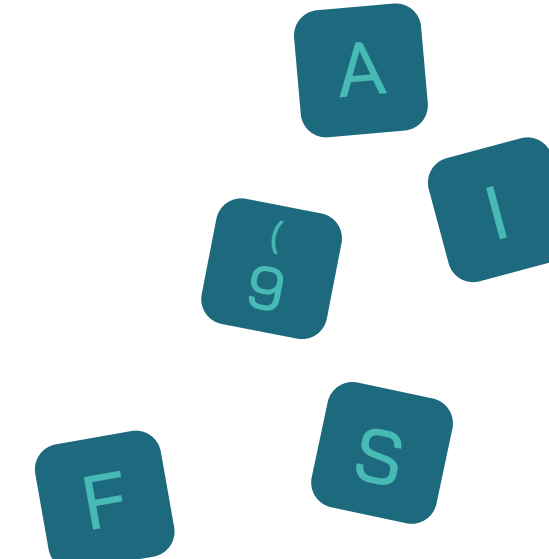
2. Meld het misdrijf
Afhankelijk van het misdrijf waarvan u slachtoffer bent geworden is het belangrijk om dit te melden bij de betrokken organisaties. Mochten cybercriminelen belangrijke bankgegevens hebben gestolen of bent uw grote geldbedragen kwijtgeraakt? Bel dan onmiddellijk de bank! Laat ze weten wat er gebeurd is. Zij hebben specialisten die u kunnen helpen om de juiste acties te ondernemen en soms de schade te beperken.

3. Doe aangifte bij de politie
Doe ook altijd aangifte bij de politie. Nu denkt u misschien dat dit toch geen nut heeft, maar dat is heeft het zeker wel! De kans is misschien klein dat uw zaak meteen wordt opgelost, maar door zaken te bundelen wordt de kans groter dat criminelen worden gepakt. Ook helpt het de politie om inzicht te houden wat er precies speelt en op deze manier kunnen anderen gewaarschuwd worden. U kunt een afspraak maken om aangifte te doen via 0900-8844.

4. Verander uw wachtwoorden
Als u uw inloggegevens heeft doorgegeven aan criminelen of u heeft bijvoorbeeld op een link geklikt tijdens een gesprek met een nep helpdesk, dan is het verstandig om uw wachtwoorden te veranderen. Zo voorkomt u dat criminelen bij andere accounts kunnen en beschermt u andere gegevens. Als u het lastig vindt om zoveel verschillende wachtwoorden te onthouden kunt u een wachtwoordkluis gebruiken. Vraag hiervoor eventueel hulp aan iemand in uw omgeving die u vertrouwt.

Kijk ook hier eens rond:
- Fraudehelpdesk.nl
- checkjelinkje.nl
- www.seniorweb.nl

Want beter begrijpen is beter beschermen!



Deze flyer is ontwikkeld in eem samenwerking tussen het Veiligheidsnetwerk Oost-Nederland en het lectoraat Maatschappelijke Veiligheid van de Hogeschool Saxion, onder financiering van de Citydeal Lokale Weerbaarheid Cybercrime in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid.