Fraude voorkomen

De feestdagen komen er aan, het aantal bezoeken op internet neemt toe, we kijken en kopen steeds vaker op het internet. Ook voor de internet criminelen is dit vaak een goede periode om hun frauduleuze handelingen uit te voeren. Lees hieronder wat de meest voorkomende vormen van internet oplichting en fraude zijn en wat u kunt doen om deze te voorkomen.

Virussen

Virussen worden meestal verspreid via bijlagen in e-mails. Virussen zijn schadelijk, je computer wordt langzamer en jouw gegevens kunnen gewist of gestolen worden. Zorg voor een goede virusscanner op je computer, die beschermt je tegen de meeste varianten.

Oplichting bij Marktplaats

Voorkom dat je opgelicht wordt via Marktplaats. Let op:
-Betaal via de mogelijkheden die Marktplaats biedt of maak zelf het geld over.
-Een betaallink waarop je kunt tikken kan vals zijn!
-Stuur nooit een foto van je ID bewijs of bankpas.
-Voor normale betalingen is het nooit nodig om eerst een cent over te boeken, nooit eerst zelf betalen voordat je iets kan ontvangen!
-Bescherm je telefoonnummer, e-mailadres en woonadres om identiteitsfraude te voorkomen.
Weet je wat jouw onderbuikgevoel is:
Als je onderbuikgevoel zegt “het voelt niet goed” , dan zou het zo maar kunnen dat dit inderdaad geen zuivere koffie is. Controleer dan altijd of het klopt.
Overbieden of direct ophalen kan een slechte voorbode zijn.

Whatsappfraude met een hulpvraag (vriend-in-Nood)

Maak altijd afspraken over betaalverzoeken met je familie en vrienden om te voorkomen dat je slachtoffer van fraude wordt. Krijg je een financiële hulpvraag, bel dan altijd eerst met die persoon met het bij **jouw** bekende nummer en vooral niet het nieuwe nummer wat wordt doorgegeven.
AIs die persoon niet direct te bereiken is, dan maak je geen geld over voordat je hem of haar hebt gesproken. Niet gesproken betekent geen geld overboeken!

Phishing

Phishing zijn nepberichten waarmee een oplichter achter jouw wachtwoorden en inlogcodes probeert te komen.
Bijvoorbeeld door jou op een bepaalde link te laten klikken. Phishing berichten krijg je vaak per e-mail of SMS. Je komt dan vaak naar een goed nagemaakte website geleid.
Hoe kan je Phishing berichten herkennen:
-Wordt je onder druk gezet om geld over te maken of codes door te geven? Grote kans dat je te maken hebt met criminelen.
-Controleer het e-mailadres van de afzender.
-Let op: banken sturen nooit linkjes naar een inlogpagina. Tik altijd zelf het webadres in.
-Vertrouw je een e-mail van je bank niet, vraag het na bij de bank en verwijder de e-mail.
-As je toch iets hebt aangeklikt of gegevens hebt ingevuld bel je bank en blokkeer desnoods je rekening of betaalpas.

Gijzelsoftware

Klik je op een link in een Phishingmail? Dan kun je zonder dat je het zelf doorhebt gijzelsoftware installeren op je computer. Dit wordt ook wel Ransomware genoemd. De oplichter zet je bestanden achter slot en grendel en vraagt om losgeld voordat je jouw bestanden weer kunt gebruiken. Toch is het maar de vraag of je de ontgrendel code echt krijgt als je betaalt. Nooit betalen dus, maar probeer je computer te laten herstellen door een erkend bedrijf.

Bankhelpdeskfraude (Spoofing)

Bij Spoofing wordt je gebeld door iemand die zich voordoet als een medewerker van de bank. Zorg dat je hier geen slachtoffer wordt. Tips:
-Uw bank vraagt nooit om geld over te boeken, je pincode te geven, je bankpas af te geven of de medewerker mee te laten kijken op je computer. Bewaar je pincode geheim en maak nooit zomaar geld over. En je bankpas? Je bank vraagt nooit om je bankpas met de post te versturen. Natuurlijk komt komt er ook geen medewerker uw pas ophalen.
-Twijfel je over een telefoontje of sms van de bank, omdat je gevraagd wordt om geld over te maken? Hang op, klik weg en bel je bank zelf via het nummer dat staat op de officiële website van je bank. Een echte bankmedewerker vindt dit echt geen probleem!

De zogenaamde geldezels

Criminelen op het internet maken gebruik van mensen die het gestolen geldbedrag kunnen wegsluizen naar een vreemde rekening. Hoe doen ze dat? Door te vragen of ze snel geld willen verdienen en wat geld op jouw rekening te laten storten. Deze persoon, dus de geldezel, pint dit bedrag en geeft het contant aan de crimineel of leent hem even zijn pinpas met pincode.

Zorg dat je hier niet intrapt; onthoud:
-Is een verhaal te mooi om waar te zijn, dan is dit het ook. Vooral ook tijdelijk geen geld op jouw rekening laten storten.
-Ga er niet op in en geef nooit jouw bankrekening of bankpas uit handen. Jouw betaalpas is persoonlijk. Voelt dit niet goed, meldt dit bij de bank en politie.

Wat kunt u zelf doen?

Houdt altijd uw codes voor iedereen geheim en geef uw bankpas nooit aan anderen.
Zorg voor een goede beveiliging van uw apparaten en smartphone.
Bekijk met grote mate uw afschriften of rekeningen.
Houdt uw pinlimiet zo laag mogelijk.
Lees de informatie over veilig bankieren bij uw bank of op de website www.veiligbankieren.nl