1. Identiteitsfraude

Bij identiteitsfraude maakt iemand misbruik van de persoonsgegevens van een ander, met de bedoeling hiermee verboden handelingen te verrichten. Bijvoorbeeld op een valse naam spullen kopen en niet betalen.

1.1 Hoe voorkom je fraude met een kopie?

Geef nooit zomaar jouw identiteitsbewijs af. Als iemand een kopie wil maken, vraag dan altijd waarom dit nodig is. Registratie van het soort identiteitsbewijs en het documentnummer is meestal voldoende. Bijvoorbeeld: 'Paspoort, NWLFR3706.' Geef je een kopie af? Help dan misbruik te voorkomen.

Schrijf op de kopie

- dat het een kopie is;
- voor wie of welk product de kopie bedoeld is;
- de datum waarop je de kopie afgeeft.

Streep jouw burgerservicenummer door in het document zelf, maar ook in de strook nummers onderaan. Jouw BSN is een persoonsnummer waarvan het gebruik aan strenge regels is gebonden. Maakt een bedrijf of organisatie een kopie van jouw identiteitsbewijs, dan is de kans groot dat dit bedrijf of deze organisatie jouw BSN niet mag hebben. Er is een lijst van organisaties/bedrijven die het BSN mogen gebruiken. Deze lijst is te vinden op http://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/documenten-en-publicaties/publicaties/2013/01/23/overzicht-organisaties-die-het-burgerservicenummer-gebruiken.html.

1.2 Ben ik verplicht om een kopie van mijn identiteitsbewijs te geven aan een bedrijf?

Nee, alleen in uitzonderlijke gevallen ben je verplicht een kopie van jouw identiteitsbewijs te laten maken. Jouw werkgever is bijvoorbeeld verplicht een kopie van jouw identiteitsbewijs bij de loonadministratie te bewaren. Het bedrijf of organisatie moet je informeren over de wettelijke verplichting.

1.3 ID-cover

De ANWB is enige tijd geleden begonnen met de verkoop van de ID-cover, een speciaal hoesje voor het paspoort, identiteitskaart en rijbewijs dat de foto en het Burger Service Nummer afdekt, wat het risico op identiteitsdiefstal moet verkleinen.

1.4 Overige bronnen/meer info:

- http://www.rijksoverheid.nl/nieuws/2013/01/10/laat-u-niet-zomaar-kopieren-voorkom-fraude-met-een-kopie-van-uw-identiteitsbewijs.html
- http://www.rijksoverheid.nl/nieuws/2013/01/15/campagne-tegen-identiteitsfraude.html
- http://www.mijnprivacy.nl/Nieuws/Pages/20120712_gebruik-kopie-identiteisbewijs.aspx
- http://www.overheid.nl/identiteitsfraude/identiteitsfraude-melden
- http://www.rijksoverheid.nl/onderwerpen/paspoort-en-identificatie/vraag-en-antwoord/hoe-kan-ik-mezelf-beschermen-tegen-identiteitsfraude.html
- http://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/documenten-en-publicaties

- http://webwinkel.anwb.nl/webwinkel/reisartikelen/id-cover-id-kaart.html (n.b.: ook voor ID-kaarten afgegeven vóór 20-10-2011 is een cover beschikbaar)

2. Internetfraude

Internetfraude is oplichting via het internet.

Enkele voorbeelden van internetfraude:
- Identiteitsfraude, reeds besproken onder 1;
- Voorschotfraude;
- Phising, zie verder onder 3;
- Valse liefde / valse vriendschap / romantische fraude;
- Nigeriaanse oplichting;
- Goederen kopen / verkopen op het internet

2.1 Bronnen/meer info:

- http://www.opgeletopinternet.nl/
- https://www.mijnpolitie.nl/if.shtml
- https://www.mijnpolitie.nl/b/miocheck2.html
- http://www.vergelijkinternetbetalen.nl/nieuwegoederen.html
- http://lexx-it.nl/lexxit-knowledge/oplichting-op-internet-internet-fraude/
- http://plazilla.com/page/4295114559/wat-zijn-voorbeelden-van-internetfraude
- http://nl.wikipedia.org/wiki/Internetfraude
- http://www.digibewust.nl/
- https://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Softwarelekken/WD-2014-006+Waarschuwing+phishing-e-mail+van+rijksoverheidnl+over+non-actiefzetting+van+uw+bank+account.html

3. Phishing

Phishing is de verzamelnaam voor alle digitale activiteiten waarmee criminelen proberen om jou persoonlijke informatie te ontfutselen. Met deze informatie kan fraude met internetbankieren, pinpassen, creditcards of jouw identiteit worden gepleegd. Phishing is vaak gericht op een grote groep personen, maar kan ook specifiek op één persoon of een kleine groep zijn gericht. Hierbij wordt gebruik gemaakt van informatie die al van de persoon of groep bekend is, zoals het e-mailadres, de naam of de functie.

3.1 Phishing: Werkwijze crimineel

Phishing gebeurt zowel per telefoon als per e-mail. Hierbij doet de crimineel zich voor als betrouwbare instantie. Zo kun je een e-mail krijgen die van jouw bank afkomstig lijkt, met het verzoek om voor controle persoonlijke gegevens, zoals jouw naam, adres, telefoonnummer, rekeningnummers en beveiligingscodes in te voeren op een website. In sommige gevallen kan de crimineel hiermee al misbruik maken van jouw rekening. Ook kan je worden gevraagd een telefoonnummer te bellen, omdat anders jouw rekening geblokkeerd wordt.

In andere gevallen kan de crimineel met de verkregen informatie jouw later bellen en zich voordoen als bankmedewerker. Hij of zij vraagt dan bijvoorbeeld om jouw beveiligingscodes, omdat er problemen zouden zijn met jouw rekening en de medewerker wil controleren of alles in orde is.

3.2 Phishing: Wat kun je doen?

Wees je ervan bewust dat criminelen op jouw gegevens uit kunnen zijn. Wees altijd heel kritisch vóór je (persoonlijke) gegevens afgeeft. Gebruik voor hulp hierbij de Spoedcursus online zelfverdediging. Bedenk dat jouw bank je nooit zal vragen om beveiligingscodes op onverwachte momenten of plekken, dus nooit per e-mail en nooit per telefoon. Daarnaast is het verstandig gebruik te maken van een spamfilter. E-mails waarover je twijfelt moet je meteen verwijderen. Heb je onverhoopt toch persoonlijke gegevens gegeven aan een phisher of stuit je op onverwachte zaken bij het internetbankieren? Meld dit dan direct bij jouw bank.

3.3 Zo kun je phishing onder andere herkennen:

- Een onverwachte e-mail van jouw eigen, andere bank of Nederlandse Vereniging van Banken (NVB), waarin je wordt gevraagd naar beveiligingscodes en/of persoonlijke gegevens.
- Taalkundig slecht geschreven e-mails.
- De e-mail is niet aan jou persoonlijk gericht.
- In de e-mail vraagt de beveiligingsafdeling van jouw bank of NVB jou iets te doen.
- Er wordt gevraagd naar beveiligingscodes en/of persoonlijke gegevens
- Er wordt gedreigd met gevolgen als je niet direct reageert.
- Je wordt gevraagd op een link te klikken naar een vreemde website.
- Je wordt gevraagd de e-mail te beantwoorden met persoonlijke gegevens.
- Jouw mailprovider of spamfilter heeft een indicatie van ‘spam’ gegeven.
- In plaats van mailtjes met tekst, versturen de internetcriminelen de phishingmails vaak met plaatjes met tekst. Dit wordt gedaan om spamfilters te omzeilen. Deze mails zijn te herkennen doordat je de tekst (afzonderlijke woorden) niet kunt selecteren met de muis.
- Jouw bank of NVB stuurt je hoogst zelden mails voorzien van bijlagen. Ontvang je dan ook een mail met bijlagen zogenaamd van jouw bank of NVB, open deze dan niet en zeker geen bijlagen met de extensie '*.exe*'.
- Kijk naar de afzender van de mail (bovenin de mail). Staat er na '@' wel de juiste naam van jouw bank, dus de naam van de site waar je altijd op inlogt? Dus bijvoorbeeld abnamro.nl, rabobank.nl of ing.nl? Nee, gooi deze mail dan direct weg.

Voorbeelden van phisingmails zijn te vinden op:

https://www.veiligbankieren.nl/nl/internetbankieren/phishing/voorbeelden-phishingmails.html

3.4 Bronnen/meer info:

https://www.veiligbankieren.nl/nl/internetbankieren/phishing.html

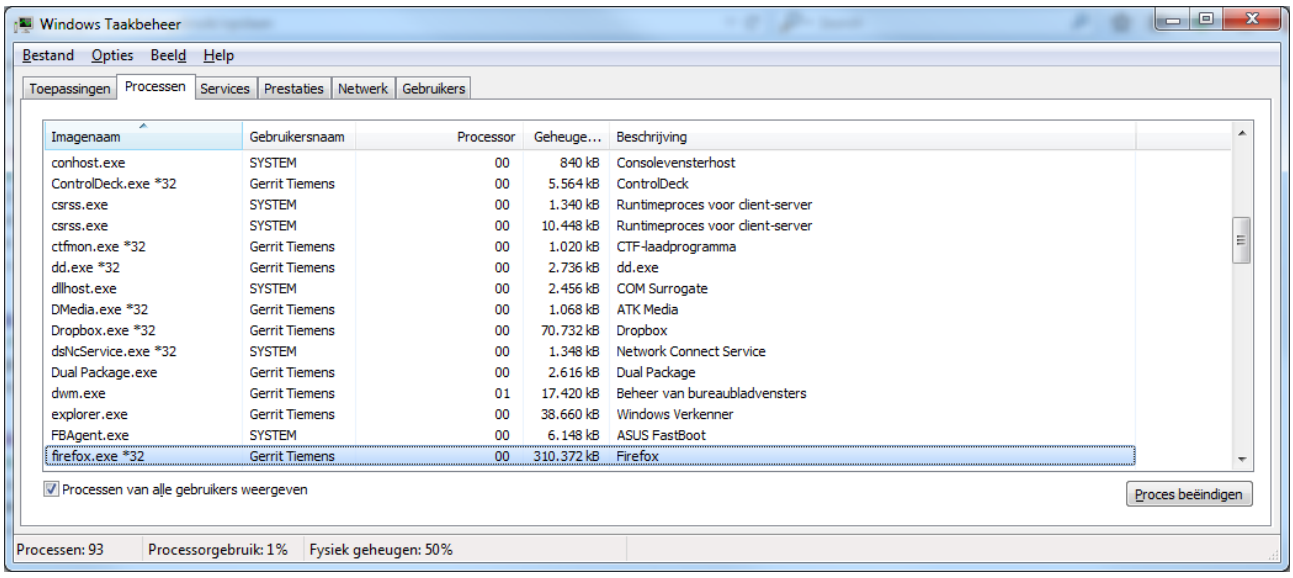
4. Speciaal

Politie (CYBERCRIME POLITIE NEDERLAND) Virus "Uw persoonlijke computer wordt geblokkeerd"

Boodschap die het computerscherm van de gebruiker blokkeert en die zogenaamd gestuurd wordt door het Korps Landelijke Politiediensten (Openbaar Ministerie, CYBERCRIME POLITIE NEDERLAND). Dit is een vorm van oplichting. Dit bericht wordt niet door een Nederlandse autoriteit gestuurd. Het is een gijzelvirus, ook wel ransomware genoemd, dat gemaakt werd door Cybercriminelen met als doel nietsvermoedende Nederlandse PC-gebruikers ertoe te verleiden een boete van 100 Euro te betalen (met PyaSafeCard of Ukash). Dit

schermblokkerende bericht stelt dat de PC gebrukers een boete moeten betalen voor het bekijken van pornografie of het gebruik van auteursrechtelijk beschermde muziek, video's of software.

Wat te doen zodra deze melding in de browser verschijnt? Start Taakbeheer, selecteer het tabblad Processen en zoek de browser op.



Kies vervolgens voor 'Proces beëindigen'. Het kan voorkomen dat de browser meerdere keren voorkomt in het overzicht (bijv. Google Chrome). Zorg ervoor dat de cache van de browser leeggemaakt wordt. Dat kan bijv. met Ccleaner. Start daarna de browser weer op. Als dan

gevraagd wordt om de vorige situatie te herstellen, kies dan voor 'nee'.