Checklist Internetoplichting

Phishing, voorschotfraude en identiteitsfraude; zomaar een aantal vormen van internetoplichting waar u slachtoffer van kunt worden. Steeds meer mensen internetten, en online zijn wordt steeds belangrijker. Criminelen merken dit ook en proberen u op slinkse wijze online te verleiden tot nepaankopen of het overmaken van geld. In de Checklist Internetoplichting zetten wij samen met Fraudehelpdesk een aantal veelvoorkomende vormen van internetoplichting op een rij.

Phishing

- ☐ Wat is het?
- ☐ Wat zijn de kenmerken?
- ☐ Hoe voorkomt u dat u slachtoffer wordt?
- ☐ Wat te doen als u slachtoffer bent geworden?

Voorschotfraude

- ☐ Wat is het?
- ☐ Wat zijn de kenmerken?
- ☐ Hoe voorkomt u dat u slachtoffer wordt?
- ☐ Wat te doen als u slachtoffer bent geworden?

Microsoft-telefoontjes

- ☐ Wat is het?
- ☐ Wat zijn de kenmerken?
- ☐ Hoe voorkomt u dat u slachtoffer wordt?
- ☐ Wat te doen als u slachtoffer bent geworden?

Identiteitsfraude

- ☐ Wat is het?
- ☐ Wat zijn de kenmerken?
- ☐ Hoe voorkomt u dat u slachtoffer wordt?
- ☐ Wat te doen als u slachtoffer bent geworden?

Handige links

Phishing

Wat is het?

De term phishing komt van het Engelse 'fishing', wat 'vissen' betekent. Het gaat namelijk om een vorm van internetfraude waarbij gehengeld (gevist) wordt naar inloggegevens, betaalgegevens en geld van mensen. Criminelen sturen e-mails of berichten op sociale media naar willekeurige mensen. Via deze berichten proberen ze u naar een website te lokken waar u uw inloggegevens (van bijvoorbeeld uw bank) moet invullen. De website waarnaar u wordt doorgelinkt lijkt een echte website, maar is helaas een nepwebsite. Zodra u inlogt, worden uw inloggegevens doorgestuurd naar de criminelen achter de nepwebsite. Met behulp van deze gegevens proberen ze uw bankrekening te plunderen.

Phishing gebeurt echter niet alleen via e-mail. Veel oplichters sturen ook brieven in plaats van een e-mail. Deze brieven zien er professioneel uit en bevatten het logo en adres van bijvoorbeeld de bank. De criminelen sturen soms ook retourenveloppen mee zodat u onder andere uw pinpas en pincode kunt opsturen. Een andere manier die oplichters gebruiken om achter uw gegevens te komen, is via de telefoon. Ze bellen op en zeggen bijvoorbeeld dat ze van Microsoft zijn en u willen helpen met het verhelpen van een probleem op uw computer. En sinds kort worden er ook sms'jes verstuurd die leiden naar nepwebsites of die u proberen te verleiden een duur sms-abonnement af te sluiten.

Wat zijn de kenmerken?

Het is steeds lastiger om een phishingmail te herkennen aan het gebrekkige Nederlands. Criminelen maken namelijk steeds betere e-mails. U moet nu dus beter lezen en kijken dan vroeger, om te zien of het om een valse mail gaat. Veel phishingmails kunt u echter herkennen aan één of meerdere van de volgende kenmerken:

- ☑ Er is sprake van een algemene aanhef, bijvoorbeeld ‘Geachte klant’.
- ☑ Er wordt gevraagd om op een link te klikken, inlogcodes te geven of geld te betalen.
- ☑ De mail is slecht geschreven. Denk aan slechtlopende zinnen en spel- en grammaticafouten, of er worden Engelse woorden gebruikt.
- ☑ Het gaat vaak om een dringend verzoek; u wordt gevraagd snel te reageren want anders zal het vervelende gevolgen hebben.
- ☑ Er wordt beweerd dat uw rekening is geblokkeerd of dat dit gaat gebeuren. Door paniek te zaaien hopen de oplichters dat u impulsief reageert en de door hen gewenste informatie verstrekt.
- ☑ De mailadressen van de afzenders wijken af van het adres van de organisatie die de mail zou hebben verstuurd. Dit kunt u zien door met de muis op het adres te staan zonder erop te klikken.
- ☑ Er staat een link in de mail, die verwijst naar een andere website dan naar de site van bijvoorbeeld uw bank. U kunt een foute link herkennen door met de muisaanwijzer op de link te gaan staan, zonder erop te klikken. Gebruikt u webmail dan ziet u het webadres nu linksonder in beeld. Gebruikt u een mailprogramma op de pc, dan ziet u het webadres in een klein pop-upje. Bekijkt u de mail op de tablet dan kunt u dit trucje ook toepassen. Houd uw vinger wat langer op de URL totdat de link in beeld verschijnt. Ziet het webadres er vreemd uit en verwijst het niet naar de website die u verwacht? Dan betreft het een phishingmail.

Hoe voorkomt u dat u slachtoffer wordt?

Vindt u het lastig om op basis van bovenstaande punten een phishingmail te herkennen? Onthoud dan in ieder geval onderstaande punten, dan is de kans dat u slachtoffer wordt van een valse mail al een stuk kleiner:

- ☑ Verstrek nooit per telefoon of e-mail persoonlijke gegevens zoals een bankrekeningnummer, pasnummer, pincode, betaalcode of persoonsgegevens zoals naam, geboortedatum of adres. Medewerkers van banken en andere instellingen vragen nooit telefonisch of via de mail naar dit soort informatie.
- ☑ Kijk naar de afzender van de mail. Staat er na '@' de juiste naam van uw bank, dus de naam van de site waar u altijd op inlogt zoals abnamro.nl, rabobank.nl of ing.nl? Nee? Gooi de mail direct weg.
- ☑ Ga nooit via een link in een mail naar de website van de bank. Gebruik daarvoor uw internetprogramma zoals Internet Explorer of Chrome en surf zelf naar het bekende webadres.
- ☑ Controleer of er een 's' staat achter de 'http'-adresregel van de website. De 's' staat voor 'secure', wat 'veilig' betekent. Als een site met 'https' begint, is er sprake van een beveiligde verbinding.
- ☑ Controleer of uw browser bij de website, in de adresbalk, het symbool 'hangslot gesloten' () weergeeft.
- ☑ Bescherm de computer tegen virussen, spyware en hackers met een up-to-date antivirusprogramma.
- ☑ Wees voorzichtig met het downloaden van programma's. Download nooit illegale programma's.
- ☑ Wees altijd alert op onbekende bijlagen in e-mails. Klik nooit op bijlagen in een mail die u van onbekenden hebt gekregen, en pas zelfs bij mails van bekenden goed op.

Wat te doen als u slachtoffer bent geworden?

Bent u bang dat u gegevens hebt ingevuld op een nepwebsite? Dan kunt u het beste zo snel mogelijk contact opnemen met uw bank of de betrokken organisatie. Doe dit dan wel via de contactgegevens op de website van de organisatie in plaats van via de contactgegevens in de mail.

Daarnaast kunt u bij Fraudehelpdesk (www.fraudehelpdesk.nl) melding maken van de situatie. De Fraudehelpdesk geeft u waar nodig advies over eventuele verdere stappen en bij het doen van aangifte.

Let op: door simpelweg te klikken op een link in een phishingmail bent u niet direct slachtoffer van phishing. Pas wanneer u persoonlijke gegevens hebt ingevuld of geld hebt overgemaakt, moet u actie ondernemen. Een mail kan als bijlage echter ook virussen of malware bevatten. Gelukkig beschermt een up-to-date virusscanner, de computer tegen de meeste bedreigingen. Maar een garantie hebt u nooit, dus het beste is om nooit zomaar op links en bijlagen in e-mails te klikken.

Voorschotfraude

Wat is het?

Voorschotfraude is een fraudevorm waarbij criminelen u iets waardevols aanbieden. Voordat u dit bedrag of product overhandigd krijgt, moet u echter eerst (relatief) kleine onkosten voorschieten. Zodra u geld overmaakt, lopen de bedragen steeds verder op. Totdat u uiteindelijk enorme bedragen kwijt bent of totdat u zelf afhaakt. Dit afhaken proberen de fraudeurs echter te voorkomen door mooie verhalen te vertellen of door zelfs dreigementen te gebruiken. Deze vorm van fraude wordt ook wel Nigeriaanse fraude genoemd.

Er zijn verschillende vormen van voorschotfraude bekend. Wij behandelen een aantal veelvoorkomende vormen. Bij alle vormen wordt er, op slinkse wijze, gevraagd geld over te maken. Geld dat u vervolgens nooit meer terugziet.

Datingfraude

Datingfraude is een van de vormen van voorschotfraude. Bij datingfraude maken fraudeurs misbruik van mensen die via datingsites op zoek zijn naar een nieuwe relatie. Maar niet alleen relatiezoekenden worden benaderd. Datingfraudeurs benaderen ook steeds vaker zomaar mensen via sociale media zoals Facebook. Vaak doen deze datingfraudeurs zich voor als een Britse of Amerikaanse zakenman of militair die voor zijn werk in West-Afrika of Afghanistan zit. Om een betrouwbare en eigen identiteit te creëren, worden foto's van internet gehaald en toegevoegd aan het profiel.

Een datingfraudeur speelt, nadat het eerste contact is gelegd, in op de gevoelens van het potentiële slachtoffer. Daarnaast zal de fraudeur voorstellen de datingsite te verlaten, en via bijvoorbeeld e-mail, WhatsApp of Skype contact te hebben. Door het contact van de datingsite te verplaatsen naar een ander medium, omzeilt de fraudeur namelijk de controles van datingsitebeheerders.

Wanneer er eenmaal sprake is van een relatie of verliefdheid, wordt er vrij snel om geld gevraagd door de fraudeur. Bijvoorbeeld om zijn nieuwe liefde te ontmoeten of vanwege een noodgeval, zoals een bezoek aan het ziekenhuis. Kortom, allemaal smoezen om geld los te peuteren bij zijn 'geliefde'.

Zodra de fraudeur het idee heeft dat het slachtoffer grotere financiële reserves heeft, wordt de fraudevorm vaak uitgebreid. Hierbij kan gedacht worden aan zogenaamde investeringsmogelijkheden, veilig te stellen erfenissen en weg te smokkelen goud, geld of juwelen. Het komt zelfs voor dat het slachtoffer de vraag krijgt geld van andere slachtoffers via de eigen rekening over te maken naar een andere bank.

In onderstaande tabel ziet u de kenmerken van datingfraude, vindt u tips om te voorkomen dat u slachtoffer wordt en ziet u wat u moet doen als u slachtoffer bent geworden.

Wat zijn de kenmerken?	Een datingfraudeur: ☑ dringt aan de datingwebsite te verlaten voor een ander communicatiekanaal (bijv. e-mail, Skype of WhatsApp). ☑ verklaart onmiddellijk zijn liefde. ☑ is bovengemiddeld attent. ☑ spreekt of schrijft doorgaans gebrekkig Engels. ☑ beweert Amerikaans/Brits of militair te zijn en is vertrokken naar of werkt in het buitenland. ☑ maakt plannen om het slachtoffer te bezoeken, maar is niet in staat dit te doen vanwege een tragische gebeurtenis.

	☑ vraagt om geld voor bijvoorbeeld reizen, medische noodgevallen, hotelrekeningen, ziekenhuisrekeningen voor een kind of ander familielid, visa of andere officiële documenten. ☑ vraagt om betalingen te doen via Western Union of MoneyGram en meestal moet dit snel gebeuren. ☑ stuurt foto's die van internet zijn geplukt. Op het tabblad 'Afbeeldingen' in Google kunt u, door de foto in de zoekbalk te slepen, controleren of de foto vaker voorkomt op internet.
Hoe voorkomt u dat u slachtoffer wordt?	☑ Wees alert op zielige verhalen. Vraag u af waarom u degene bent die de financiële ondersteuning moet geven in plaats van familie, vrienden of een werkgever. ☑ Controleer de naam en eventuele foto's van de datingpartner op internet. Maar als er geen informatie opduikt, betekent dit niet automatisch dat iemand ook te vertrouwen is. Op het tabblad 'Afbeeldingen' in Google kunt u, door de foto in de zoekbalk te slepen, controleren of de foto vaker wordt gebruikt op internet. ☑ Ga niet op het voorstel in om de datingsite te verlaten om op een andere manier met elkaar te communiceren. ☑ Breng uzelf en uw identiteit niet in gevaar door te snel op mensen te vertrouwen. Wees voorzichtig als u nieuwe mensen leert kennen. ☑ Vertrouw op uw intuïtie. ☑ Wees wantrouwend ten opzichte van datingpartners die zich niet in Nederland bevinden. ☑ Check eventueel bij het bedrijf of de organisatie waar de datingpartner 'werkt' of zijn verhaal klopt. ☑ Vertrouw niet blindelings op formulieren die er mooi en professioneel uitzien. ☑ Onderzoek of het (vaak gebrekkige) taalgebruik wel overeenkomt met de 'status' van de datingpartner. ☑ Sta uiterst wantrouwig tegenover het (plotseling) opduiken van bijvoorbeeld investeringsmogelijkheden, erfenissen, goud, juwelen of grote sommen geld die moeten worden weg gesmokkeld. ☑ Maak nooit geld over naar iemand die u niet in het echt hebt ontmoet. ☑ Maak absoluut geen gebruik van Western Union, MoneyGram of een ander geldkantoor. Deze bureaus staan erom bekend voor oplichtingspraktijken te worden gebruikt. ☑ Praat met iemand over uw nieuwe partner.
Wat als u slachtoffer bent geworden?	☑ Neem contact op met Fraudehelpdesk. ☑ Doe aangifte bij de politie. Laat in de verklaring opnemen dat u zich opgelicht voelt en dat u nooit geld zou hebben betaald als u had geweten dat alles een grote leugen was. Eis in de aangifte het geld terug van de oplichter. ☑ Verbreek ieder contact met de fraudeur. Blokkeer dus ook de e-mailadressen en telefoonnummers. ☑ Laat de datingsite weten dat u bent opgelicht zodat het account van de fraudeur kan worden verwijderd. ☑ Praat met iemand over wat er met u is gebeurd. Uw vertrouwen is geschaad en dat moet u verwerken.

Erfenisfraude

Erfenisfraude is ook een vorm van voorschotfraude. Bij erfenisfraude sturen fraudeurs een brief of e-mail met daarin het nieuws dat er een erfenis is vrijgekomen van een ver familielid of naamgenoot. De ontvanger van deze brief of e-mail erft zogenaamd (een deel van) een grote erfenis. Om het verhaal zo geloofwaardig mogelijk te maken, voegen de fraudeurs authentiek lijkende certificaten en documenten toe.

Zodra het vertrouwen van de ontvanger is gewonnen, vraagt de fraudeur om geld over te maken. Het bedrag dat overgemaakt dient te worden zijn "kosten die noodzakelijk zijn om het geld vrij te maken". Dit zijn in het begin kleine bedragen, maar de kosten worden steeds hoger. Aan het einde van de rit wordt er geen erfenis uitgekeerd, omdat deze niet bestaat. Het overgemaakte geld is naar de oplichter gegaan.

In onderstaande tabel ziet u de kenmerken van erfenisfraude, vindt u tips om te voorkomen dat u slachtoffer wordt en ziet u wat u moet doen als u slachtoffer bent geworden.

Wat zijn de kenmerken?	☑ Er wordt een grote erfenis in het vooruitzicht gesteld. ☑ De documenten en/of personen die u benaderen komen uit Nigeria of andere West-Afrikaanse landen, of uit Engeland, Spanje, Zuid-Amerika, Roemenië, Rusland of Oekraïne. ☑ De e-mailadressen van de afzenders zijn algemene e-mailadressen zoals Gmail, Hotmail en Yahoo. ☑ De correspondentie is in gebrekkig Engels. ☑ De documenten staan vol taal- en spelfouten. ☑ Digitaal doorgezonden 'officiële' documenten worden als Word-documenten verzonden. ☑ U krijgt de vraag geld over te maken.
Hoe voorkomt u dat u slachtoffer wordt?	☑ Maak nooit geld over dat nodig zou zijn om een groot bedrag in handen te kunnen krijgen. Vraag desnoods het geld in mindering te brengen op het vrijgegeven bedrag. Kan dit niet, dan weet u al genoeg! ☑ Doe nooit zaken met officiële instanties als die gebruikmaken van algemene e-mailadressen zoals Gmail, Hotmail en Yahoo. ☑ Laat aangeboden documenten controleren op echtheid door bijvoorbeeld een ambassade of de Marechaussee. ☑ Stuur dit soort mails door naar het abuse-adres* van uw provider.
Wat te doen als u slachtoffer bent geworden?	☑ Doe aangifte bij de politie. ☑ Neem contact op met Fraudehelpdesk.

* Een abuse-adres is een e-mailadres (in dit geval van uw provider) waar u misbruik kunt melden. Voorbeelden van abuse-adressen zijn: abuse@kpnmail.nl, abuse@ziggo.nl en abuse@zeelandnetbv.nl.

Loterijfraude

Een derde vorm van voorschotfraude is loterijfraude. Met een telefoontje, e-mail of sms met daarin de boodschap dat er een groot geldbedrag gewonnen is in een loterij, proberen loterijfraudeurs u te misleiden. Om de prijs te ontvangen moet u contact opnemen met de organisatie. Om het verhaal geloofwaardig te maken, tonen de oplichters vaak authentiek lijkende certificaten en documenten.

Wie ingaat op deze berichten, krijgt al snel het verzoek een bedrag over te maken voor kosten die zogenaamd noodzakelijk zijn om het geld te ontvangen. Net zoals bij andere vormen van voorschotfraude gaat dit in eerste instantie vaak om kleine bedragen, die steeds

verder oplopen. Het geld dat het slachtoffer overmaakt, is hij/zij kwijt en de hoofdprijs wordt niet uitgekeerd.

Daarnaast kunnen loterijfraudeurs onder meer vragen om persoonlijke informatie of kopieën van officiële documenten, zoals uw paspoort of rijbewijs. Deze gegevens zijn zogenaamd nodig om uw identiteit te bevestigen. De fraudeurs kunnen deze informatie echter gebruiken om identiteitsfraude te plegen. Wat dit precies is, leest u verderop in deze checklist.

In onderstaande tabel ziet u de kenmerken van loterijfraude, vindt u tips om te voorkomen dat u slachtoffer wordt en ziet u wat u moet doen als u slachtoffer bent geworden.

Wat zijn de kenmerken?	☑ Er wordt een grote prijs in het vooruitzicht gesteld. ☑ Er wordt gebruikgemaakt van de naam van een bestaande loterij of organisatie zoals Google of Microsoft. ☑ De mail komt uit het buitenland. ☑ De e-mailadressen van de afzenders zijn algemene e-mailadressen zoals Gmail, Hotmail en Yahoo. ☑ De e-mail is in slecht Engels geschreven. ☑ De documenten staan vol taal- en spelfouten. ☑ De 'officiële' documenten worden als Word-bestand verzonden. ☑ U krijgt de vraag geld over te maken.
Hoe voorkomt u dat u slachtoffer wordt?	☑ Maak nooit geld over om een groter bedrag in handen te krijgen. ☑ Ga niet in op organisaties die gebruikmaken van algemene e-mailadressen zoals Gmail, Hotmail en Yahoo. ☑ Laat documenten controleren door bijvoorbeeld de ambassade of de Marechaussee. ☑ Stuur de mail door naar uw e-mailprovider en de loterij in kwestie zodat het bedrijf weet dat er fraudeurs actief zijn. Vergeet niet: ☑ Gratis loterijen bestaan niet. U kunt nooit een prijs winnen als u geen lot hebt gekocht. ☑ Betaal nooit om een prijs in ontvangst te nemen. Geen enkele rechtmatige loterij vraagt hierom.
Wat te doen als u slechtoffer bent geworden?	☑ Doe aangifte bij de politie. ☑ Neem contact op met Fraudehelpdesk.

Marktplaatsfraude

Bij marktplaatsfraude, ook een vorm van voorschotfraude, wordt er een product gekocht, maar gaat er uiteindelijk iets mis: u betaalt wel, maar het product wordt niet geleverd of u verkoopt iets, maar ontvangt geen geld.

Zo kunt u bijvoorbeeld een buitenlands bod op uw advertentie op Marktplaats of eBay krijgen. De koper wil betalen met een cheque of via het online betaalsysteem PayPal. Om bij te dragen aan de verzendkosten en eventuele verzekeringen betaalt de koper echter een hoger bedrag dan de afgesproken prijs, wat op het eerste gezicht een vriendelijk gebaar lijkt. De koper zal vragen het overgebleven geld (dus het geld dat overblijft na de transportkosten en eventuele verzekeringskosten) weer terug te storten naar de koper of eventueel naar een derde partij. Ter goedertrouw stort u dit bedrag terug. Achteraf blijkt echter dat de cheque of PayPal-betaling vals is. U bent dan niet alleen het product kwijt, maar ook het geld dat u terug hebt gestort naar de koper.

In onderstaande tabel ziet u de kenmerken van marktplaatsfraude, vindt u tips om te voorkomen dat u slachtoffer wordt en ziet u wat u moet doen als u slachtoffer bent geworden.

Wat zijn de kenmerken?	☑ De koper schrijft in gebrekkig Engels. ☑ De koper vraagt na de eerste contacten verder te communiceren via een ander e-mailadres. ☑ De koper woont in het buitenland, doet zich vaak voor als zakenman en wil het product kopen voor bijvoorbeeld een familielid of vriend. ☑ De koper heeft haast met de aankoop en hoeft het product niet vooraf te inspecteren. ☑ De koper wil gebruikmaken van een tussenpersoon om de betaling af te handelen (bijvoorbeeld de HSBC Bank, Citibank of PayPal). ☑ Er wordt meer geld overgemaakt dan de afgesproken prijs, zogenaamd om bij te dragen aan transportkosten en eventuele verzekeringskosten. Vervolgens wordt gevraagd het geld dat overblijft na deze kosten terug te storten naar de koper of eventueel naar een derde partij.
Hoe voorkomt u dat u slachtoffer wordt?	U koopt een product: ☑ Controleer het bankrekeningnummer van de aanbieder bij het Meldpunt Internet Oplichting. ☑ Controleer hoelang de aanbieder al actief is op de handelssite. ☑ Bekijk de andere advertenties van de aanbieder. ☑ Bekijk op internet of er informatie te vinden is over de aanbieder. ☑ Maak persoonlijk contact met de aanbieder. ☑ Betaal het liefst contant bij aflevering. ☑ Betaal nooit via anonieme betaalmethoden als Western Union of MoneyGram. ☑ Controleer op internet het bestaan van het artikel en of dat artikel niet in bezit van iemand anders is. Vaak worden foto's en gegevens gebruikt die van andere websites worden overgenomen. Bijvoorbeeld van een garagehouder, als het gaat om een aangeboden auto. ☑ Maak nooit geld over voor een artikel dat u niet live hebt kunnen aanschouwen. Ook niet aan een tussenpartij. U verkoopt een product: ☑ Laat de koper bijkomende kosten zelf regelen. Accepteer geen betaling met overwaarde. ☑ Verstuur het artikel pas als het afgesproken bedrag definitief op uw rekening staat. ☑ Wees bijzonder voorzichtig met buitenlandse bieders. ☑ Vraag u af of het wel logisch is dat men uw artikel wil kopen (vaak is het ter plekke tegen lagere kosten aan te schaffen, zeker als de bijkomende kosten als transport e.d. meegerekend worden).
Wat te doen als u slachtoffer bent geworden?	☑ Doe aangifte bij de politie. ☑ Maak melding bij de betreffende handelswebsite. ☑ Benader met uw aangifte de bank van de tegenpartij. Dat kan eventueel via uw eigen bank.

Microsoft-telefoontjes

Wat is het?

De zogenoemde Microsoftbellers zijn criminelen die de naam van Microsoft of een ander softwarebedrijf misbruiken. Ze doen zich voor als medewerkers van Microsoft die u willen helpen met bijvoorbeeld een computerprobleem. Ze komen behulpzaam over, maar zijn uit op uw geld of persoonlijke gegevens. Wie ingaat op Microsoft-telefoontjes loopt het risico dat er malware op de computer wordt geïnstalleerd. Met behulp van deze malware kunnen de criminelen achter persoonlijke gegevens komen. Daarnaast is het ook mogelijk dat u moet betalen om bepaalde problemen op te lossen. Wanneer u geld overmaakt, bent u dit geld kwijt.

Wat zijn de kenmerken?

Kenmerken van Microsoft-telefoontjes zijn:

- ☑ Er wordt gezegd dat er computerproblemen zijn. De bellers hebben hier een oplossing voor. Vervolgens:
  - wordt er gevraagd om naar een website te gaan om software te downloaden.
  - wordt er gevraagd om naar een website te gaan om hier persoonlijke gegevens achter te laten.
  - wordt er aangeraden om een virusscanner te kopen, hier moet u wel direct voor betalen.
- ☑ De beller spreekt vaak gebrekkig Engels met een Indiaas of Pakistaans accent.

Hoe voorkomt u dat u slachtoffer wordt?

Om te voorkomen dat u slachtoffer wordt van een Microsoft-telefoontje kunt u het beste de telefoon ophangen als u het gesprek niet vertrouwt. Microsoft zal u nooit zomaar opbellen om problemen te verhelpen. Ga daarnaast nooit in op verzoeken om software te downloaden, gegevens achter te laten, geld over te maken of iets te kopen.

Wat te doen als u slachtoffer bent geworden?

Wanneer u oplichters toegang hebt gegeven tot uw computer of denkt dat u toegang hebt gegeven, dan kunt u het volgende doen:

- ☑ Verbreek de internetverbinding van de besmette computer.
- ☑ Wijzig al uw wachtwoorden, bij voorkeur op een andere computer. Denk aan de inloggegevens van uw bank, e-mailadres en toegang van de computer zelf.
- ☑ Scan de computer met een goede virusscanner.
- ☑ Neem eventueel contact op met een ICT-specialist.
- ☑ Neem direct contact op met uw bank als er geld afgeschreven is van uw rekening, en volg de aanwijzingen van de bank.

Identiteitsfraude

Wat is het?

Bij identiteitsfraude worden met gestolen identiteitsgegevens of vervalste identiteitspapieren strafbare feiten gepleegd waarmee (veel) geld wordt verdiend. Zo kunnen criminelen met een gestolen paspoort een lening afsluiten, een huis kopen of een verkeersovertreding begaan onder de naam van iemand anders. Het slachtoffer komt er pas achter als er rekeningen voor hem of haar binnenkomen. Daarnaast kunnen criminelen ook uw handtekening vervalsen. Identiteitsfraude komt steeds vaker online voor. Het is zogenaamde diagonale fraude. Dat betekent dat zowel burgers, bedrijven als de overheid slachtoffer kunnen worden.

Wat zijn de kenmerken?

Er zijn een aantal signalen die erop kunnen wijzen dat uw gegevens in handen zijn gevallen van een fraudeur:

- ☑ U krijgt brieven van bedrijven, zoals incassobureaus, over schulden waar u niets mee te maken hebt.
- ☑ Er komen rekeningen of ontvangstbevestigingen binnen voor producten of diensten die u niet hebt besteld.
- ☑ Op uw bankafschriften komt u uitgaven tegen die u niet bekend voorkomen.
- ☑ U komt erachter dat uw gegevens bij de overheid zijn aangepast.
- ☑ U krijgt geen lening omdat er een signalering op uw naam staat bij het BKR.

Hoe voorkomt u dat u slachtoffer wordt?

Om te voorkomen dat u slachtoffer wordt van identiteitsfraude, moet u uiterst zorgvuldig omgaan met uw persoonlijke gegevens.

- ☑ Als u een kopie van uw identiteitsbewijs moet afgeven, maak het document dan onbruikbaar voor criminelen. Dit doet u door op de kopie te schrijven dat het een kopie is, voor wie de kopie bedoeld is, plus de datum. Streep daarnaast het Burgerservicenummer door (behalve bijvoorbeeld voor uw huisarts of bank, die mogen het BSN wel gebruiken). U kunt hiervoor ook de app KopieID gebruiken.
- ☑ Wees voorzichtig met persoonlijke informatie op papier.
- ☑ Houd uw persoonlijke gegevens voor uzelf en deel die niet zomaar met anderen.

Wat te doen als u slachtoffer bent geworden?

Denkt u dat u slachtoffer bent geworden van identiteitsfraude, dan zijn er een aantal zaken die u moet regelen:

- ☑ Doe aangifte bij de politie. Niet alleen als u zeker weet dat uw identiteitsdocumenten zoals een paspoort of rijbewijs gestolen zijn, maar ook als u ze kwijt bent.
- ☑ Stel uw bank en/of creditcardmaatschappij op de hoogte. U kunt uit voorzorg uw pasjes laten blokkeren. Vraag of er al ongebruikelijke transacties hebben plaatsgevonden.
- ☑ Verzamel bewijzen van de (vermoedelijke) fraude zoals kopieën van bankafschriften, brieven van incassobureaus of aanvragen van abonnementen.
- ☑ Meld de fraude bij het Centraal Meldpunt Identiteitsfraude- en fouten (CMI).
- ☑ Hebt u veel last van het feit dat u slachtoffer bent geworden? Neem contact op met Slachtofferhulp Nederland. U hoeft zich niet te schamen, want iedereen kan slachtoffer worden van identiteitsfraude.

Handige links

Instantie	URL
Fraudehelpdesk	https://www.fraudehelpdesk.nl
Politie (aangifte doen)	https://www.politie.nl/aangifte-of-melding-doen/aangifte-doen
Meldpunt Internet Oplichting	https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html
Centraal Meld- en Informatiepunt Identiteitsfraude en –fouten (CMI)	https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/documenten/formulieren/2014/10/23/meldingsformulier-identiteitsfraude
Slachtofferhulp Nederland	https://www.slachtofferhulp.nl/

Over Fraudehelpdesk

De Fraudehelpdesk wil voorkomen dat de Nederlandse bevolking slachtoffer wordt van fraude. Het doel van de Fraudehelpdesk is dan ook burgers en bedrijven weerbaarder maken tegen en behoeden voor oplichtingspraktijken en fraude. Dit doen zij door mensen bewust te maken van de risico's op fraude. Zo waarschuwt de Fraudehelpdesk op zijn website, Facebook en Twitter voor frauduleuze zaken.

Daarnaast biedt de Fraudehelpdesk fraudeslachtoffers een helpende hand door hen naar de juiste instantie te verwijzen. Zo hoeft de gedupeerde niet zelf op zoek naar het goede adres voor hulp. De Fraudehelpdesk heeft geen opsporingsbevoegdheid.

Over SeniorWeb

SeniorWeb is een landelijke vereniging met meer dan 149.000 leden, 400 cursuslocaties en 3.000 vrijwilligers. SeniorWeb is sinds 1996 actief met als doel de digitale wereld begrijpelijk te maken, zodat iedereen het gemak en het plezier van de computer en het internet kan ervaren. Dit doet de vereniging door alles stap voor stap en in begrijpelijke taal uit te leggen.

Op de website van SeniorWeb vindt u meer informatie over phishing (www.seniorweb.nl/onderwerp/spam-en-phishing). Daarnaast vindt u elke week in onze nieuwsbrief een overzicht van de belangrijkste phishingmeldingen van die week.

Lid worden van SeniorWeb

Bent u nog geen lid van SeniorWeb? Meld u dan voor slechts € 29,50 per kalenderjaar aan via www.seniorweb.nl/quiz/lid-worden en ontvang het boek *Veilig en vertrouwd online* cadeau. Als lid ontvangt u tijdschrift Enter en onze speciale ledennieuwsbrieven vol tips, kunt u onbeperkt deelnemen aan onze Online Cursussen en bij computerproblemen staan onze vrijwilligers voor u klaar.

Wilt u eerst kennismaken met SeniorWeb? Vraag dan vrijblijvend een proefexemplaar aan van tijdschrift Enter via www.seniorweb.nl/enter