DIGITALE VEILIGHEID
Veilig online blijven
“Echt of Nep?”

Online bankieren, berichten versturen, iets bestellen of informatie opzoeken: we doen steeds meer digitaal. Dat is handig, maar vraagt ook om alertheid. Want hoe herkent u een verdacht bericht, een nepwebsite of online fraude? En wat kunt u zelf doen om uw gegevens, apparaten en accounts beter te beschermen?
Hoe weet u wat echt of nep is? Vind antwoorden in deze informatie.

Deze informatie is voor senioren op initiatief van de BEL-combinatie in samenwerking met Maarten Keijzer van Blue Professionals.
En is tevens een samenvatting (naslagwerk) van de bijeenkomst ‘Veilig Online’, georganiseerd door de BEL Combinatie in samenwerking met BasBEL op 25 augustus 2026.

Inhoud

Informatie digitale veiligheid "Echt of Nep"

Deze informatie is niet bedoeld om u angst aan te jagen. Integendeel!
Alle genoemde onderwerpen worden benoemd en toegelicht om u te waarschuwen voor oplichtingspraktijken en online fraude. U wordt geadviseerd door middel van tips om zo veel mogelijk zelf fraude te kunnen voorkomen en u krijgt verwijzingen naar instanties die u verder kunnen helpen.

Babbeltrucs – Oplichters aan de deur

1. Babbeltrucs aan de deur vinden nog steeds plaats. Dit kan op veel manieren gebeuren, onder andere door een postpakketbezorger die een pakketje voor de buren heeft en aan u vraagt of u dit wilt aannemen. Maar u moet nog wel 1,30 eurocent portokosten betalen. Volgens de pakketbezorger kunt u alleen pinnen en stiekem verwisselt hij vervolgens uw pinpas.
2. Een ander voorbeeld is dat de pakketbezorger u vraagt een pakketje voor uw buren aan te nemen. Naderhand blijkt dat de buren niets hebben besteld. Enkele dagen later staat er iemand voor uw deur met de mededeling dat u een pakket heeft ontvangen maar niet heeft betaald.
3. In het filmpje heeft u meerdere soorten gezien, zoals de "verpleegkundigen die bij ouderen langskomen, maar ook de "zogenaamde brandweerman die de brandmelder komt controleren", duurzaamheidssubsidie"etc.
   Kortom: Als u het niet vertrouwt niet binnenlaten en even controleren.
4. Een andere, nog steeds voorkomende, truc is dat men aanbelt en vraagt of men mag telefoneren. Dit is een smoes! Vaak komt men met 2 personen. Als ze eenmaal binnen zijn houdt 1 persoon u bezig, de ander loopt door uw woning en probeert geld of sieraden te vinden en deze uiteraard mee te nemen.

Advies:

- Neem geen pakketjes aan die u niet besteld heeft. Maak eventueel met uw buren goede afspraken over het aannemen van een pakketje. Als u het niet vertrouwt, niets aannemen, de geadresseerde kan het altijd ophalen op een afhaalpunt.
- Betaal **NOOIT** portokosten of iets dergelijks.
- Probeer de deur niet helemaal te openen. Er zijn hele eenvoudige oplossingen om uw deur op een kier te openen.
  Kijk op https://nl.wikipedia.org/wiki/Kierstandhouder
- Als er in de avonduren iemand voor uw deur staat, probeer dan te controleren of het een bekende is. Dit kan bijvoorbeeld met een **deurspion:**
  https://www.amsterdamslotenmaker.com/kennisbank/wat-is-een-deurspion/
  Met behulp van een deurspion neemt u alvast polshoogte wie er voor uw deur staat, voordat u opent.
- Steeds vaker hebben bewoners een deurbel met camera. Als het een onbekende is, **NIET** binnenlaten: meer info op https://www.beldeur.nl/

- Als er een bekende in de avond wil langskomen, maak dan een afspraak dat men u belt als men voor de deur staat, of spreek een code af, bijvoorbeeld 2 of 3 keer kort aanbellen, dan weet u dat het iemand is die u kent.
- Kijk voor meer Babbeltrucs op https://www.zusterjansen.nl/blog/babbeltruc-voorbeelden

Kijk voor meer informatie op: https://www.politie.nl/onderwerpen/babbeltruc.html

Nepagenten

Nepagenten zijn oplichters die zich voordoen als iemand van de politie. De daders bellen mensen op, vaak ouderen, en doen zich voor als wijkagent. Soms gebruiken ze ook de naam van de wijkagent om u te misleiden.
De nep-(wijk)agenten stellen vragen over waardevolle spullen, geld of bankpassen en bieden aan die spullen veilig te bewaren. Daarna komen er inderdaad mensen aan de deur. Zij ‘legitimeren’ zich met een vals pasje als recherche. Soms hebben ze een deel van een (nep)uniform aan. Helaas zijn deze delen van een politie-uniform bij bepaalde webshops heel makkelijk te verkrijgen.

Explosieve stijging aantal nepagenten:

In **2023** waren er voor het eerst meldingen van nepagenten. Er kwamen toen **544** meldingen binnen bij de politie.
In **2024** kwamen er **8329** meldingen binnen, bijna 15 keer zoveel.
In **2025** is er sprake van gemiddeld **35 meldingen per dag**. *Eind november 2025 waren er bij de politie ruim **10.800 meldingen** binnengekomen. In heel 2025 ruim 11.000 meldingen. Het is echter het "topje" van de ijsberg. Veel slachtoffers schamen zich. Dit is niet nodig. Doe aangifte bij de politie en neem contact op met slachtofferhulp.*

Cijfers afkomstig van https://www.politie.nl/nieuws/2025/november/17/00-ruim-10.000-incidenten-met-nepagenten-in-2025.html


Verdacht telefoontje
Meerdere slachtoffers zijn gebeld door iemand die zich voordoet als agent. Deze 'agent' vertelt dat er onlangs is ingebroken in de buurt en dat er een risico bestaat dat de bewoner ook slachtoffer wordt.


Waardevolle spullen ophalen
Deze 'agent' stelt voor dat de politie langskomt om waardevolle spullen uit de woning te halen zodat deze veilig kunnen worden opgeborgen in een kluisop het politiebureau. De spullen worden vervolgens opgehaald, in enkele gevallen draagt deze nepagent zelfs een uniform.
Zo gaat de politie nooit te werk!


Waarschuw je omgeving
Deze oplichters hebben al meerdere slachtoffers gemaakt. We zien vaak dat het om ouderen gaat. Waarschuw ouderen in je omgeving voor deze oplichtingspraktijken.
Heb je info die ons onderzoek kan helpen? Tip ons! Bel 0900-8844.
Liever anoniem? 0800-7000

Tip bij nepagenten:
Als er agenten voor uw deur staan, vraag dan naar hun legitimatiebewijs, dat moeten ze altijd bij zich hebben. U sluit de deur en laat ze buiten wachten. U belt 0900-8844 en vraagt naar de meldkamer en u vraagt of het klopt dat er politie bij uw deur staat. De meldkamer roept deze agenten op en controleert het e.e.a. U hoort of het klopt en kunt ze eventueel binnenlaten.
Trouwens dit geldt ook voor meteropnemers of andere organisaties die binnen moeten zijn. ***Officiële organisaties hebben veel van hun werknemers voorzien van een ID document****. Bel gerust om het te controleren. Zoek dan wel het JUISTE nummer op via internet!!*

Let op uw bankpas

Door reorganisaties bij banken is het steeds lastiger om geld te pinnen. Er zijn echter ook winkels waar nog geldautomaten staan, bijvoorbeeld bij supermarkten. In veel gevallen kunt u dan tot € 250,= pinnen (o.a. bij Albert Heijn, Jan Linders, Jumbo, Primera, Gamma).
Als u geld moet pinnen, doe dit dan zoveel mogelijk in een winkel. Daar is veelal publiek aanwezig waardoor het veel veiliger is.
Pinnen in de winkel of bij de automaat

- Als u gaat pinnen zorg dan dat u dit veilig doet. Scherm uw pincode af en zorg dat er geen mensen mee kunnen kijken.
- Als er iemand te dicht bij u staat vraag dan of deze persoon afstand wil houden.
- Laat u **NOOIT** afleiden.
- Als u klaar bent met pinnen, berg uw pas dan goed. Als u geld heeft opgenomen doe dit dan in uw portemonnee en vertrek pas als u alles veilig opgeborgen heeft, ook als het druk is.

  Laat u niet opjagen en als u zich niet veilig voelt, pin dan op een ander moment!

Digitaal bankieren / betalen etc.

Steeds vaker wordt er gevraagd om d.m.v. een TIKKIE of een QR code te betalen. Er is veel informatie over het digitale bankieren.
Informatieve en betrouwbare websites:
Bankieren met Steffie (https://bankieren.steffie.nl/nl
Bankinformatiepunt - Hulp bij bankzaken (https://bankinformatiepunt.nl

Deze websites stellen u ook in de gelegenheid om te oefenen met bijvoorbeeld contactloos betalen, ect.

Phishing
Phishing is het 'hengelen' naar persoonlijke gegevens van mensen.
Phishing mails worden steeds professioneler en lijken bedrieglijk echt. Vroeger stonden veel phishing mails vol met taal- en spelfouten, maar dat gebeurt steeds minder.
Phishing is een vorm van cybercrime waarbij criminelen een e-mail, een WhatsApp bericht of SMS bericht, naar u verzenden om te proberen ***inloggegevens, creditcardinformatie, pincodes of andere persoonlijke gegevens van u te achterhalen***.

Een bank of andere betrouwbare instantie vraagt NOOIT per e-mail om uw persoonlijke gegevens aan ze door te geven.

Als u gebeld door uw bank, dan kunt up via uw bankapp kijken of het inderdaad de bank is die u belt. De banken die dat inmiddels hebben zijn ABN – AMRO, ING en RABO. *ASN is er mee bezig!*

Belangrijk:

Klik ook nooit op een link in de e-mail als u dit niet vertrouwt. Als u dit wel zou doen, kan er ongemerkt op uw computer een kwaadaardig programma worden geïnstalleerd.

Spoofing

We spreken van spoofing wanneer iets of iemand probeert een valse identiteit aan te nemen en zich voordoet als iets of iemand anders. Bekende voorbeelden van spoofing zijn het versturen van een e-mail vanuit een e-mailadres dat niet echt van de afzender is. Of het namaken van een website die precies lijkt op de officiële website. Omdat ondernemers vaak betaalde producten of diensten aanbieden op een website, of bijvoorbeeld facturen en offertes per e-mail versturen, maakt dat zij een aantrekkelijk doelwit zijn voor oplichters.

Maar een tweede techniek maakt het ineens nog veel moeilijker om kwaadwillende buiten de deur te houden**: Caller ID spoofing**.

Met caller ID spoofing doet iemand zich voor als een ander, door te bellen met een eigen telefoon, terwijl het telefoonnummer van een ander op het display verschijnt.

Deze techniek is al langer bekend en wordt vaak op een legale manier door bedrijven gebruikt, bijvoorbeeld om de doorkiesnummers van medewerkers af te schermen. Zij sturen dan alleen het algemene telefoonnummer mee. Een goede manier om de gewenste informatie bij de klant te krijgen.

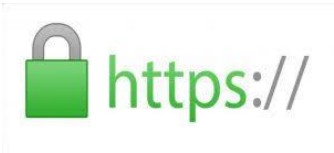
Caller ID spoofing is extreem eenvoudig toe te passen. Er zijn meerdere websites die deze dienst aanbieden. Op deze websites wordt de dienst gepromoot voor privé (“Houd je familie en vrienden voor de gek!”) en zakelijke (“Uw klanten zien alleen uw zakelijke nummer.”) doeleinden. Maar juist omdat het zo eenvoudig is, wordt er ook misbruik van gemaakt.

1 oktober 2025 in de Telegraaf:
Er zijn ongeveer 40.000 meldingen binnengekomen waarvan er 1400 slachtoffer zijn van SPOOFING. Gezamenlijk hebben zij ongeveer € 13.000.000,= schade hebben geleden.
Kijk op www.fraudehelpdesk.nl

Malware is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse malicious software (kwaadaardige software, soms schadelijke software). Malware veronderstelt kwade opzet. Software waarmee geen kwaad wordt beoogd, valt hier dus niet onder.

Kijk voor meer informatie op: https://www.digitaltrustcenter.nl/spoofing
Een betrouwbare site van het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid

Wat betekent het slotje naast de adresbalk?



Tegenwoordig zijn steeds meer websites beveiligd. Dat kunt u zien in de adresbalk van de website. Er staat dan een s (https) of zwart slotje, dit betekent dat men gebruik maakt van SLL.
SSL zorgt ervoor dat de gegevens tussen u en de webserver niet kunnen worden gestolen.

Voor meer informatie:
https://verbeterjewebsite.nl/wat-betekent-het-slotje-naast-de-adresbalk/

Melden:

Als u een phishing mail heeft ontvangen, dan kunt u dit het beste melden bij de fraudehelpdesk. Valse-mail@fraudehelpdesk.nl en u kunt deze ook doorsturen naar uw bank. Adres is: valse-email@naamvandebank.nl

Er is ook nog een leuke andere quiz over **echte of nep** berichten. Ook deze site is veilig. **Quiz echt of nep?**

Type: https://veiliginternetten.nl/quiztool/alert-online-echt-nep-quiz/
U moet de afbeelding vergroten en op alles letten. Succes.
Ook dit is een leuke kennisquiz. https://cybercrime-challenge.nl/leidse-regio/

Bankhelpdeskfraude is een vorm van spoofing die veel voorkomt en waarbij iemand in korte tijd veel geld kan kwijtraken.

Wat is bankhelpdeskfraude?

Bij deze oplichtingstruc bellen fraudeurs mensen thuis op en doen zich voor als bankmedewerkers. De slachtoffers kunnen in het beeldscherm van hun telefoon soms het daadwerkelijke nummer van de bank zien. De oplichters hebben gedetailleerde gegevens van slachtoffers, zoals rekeningnummers. Ze maken het slachtoffer wijs dat hun bankrekening niet meer veilig is. Slachtoffers krijgen daarna de vraag om zelf hun hele banksaldo met één of meer overboekingen zogenaamd ‘veilig te stellen op een kluisrekening’. Dat is uiteraard een rekening van de oplichter.

In andere gevallen komt er zogenaamd iemand van de bank de pinpas ‘met spoed’ bij iemand thuis ophalen en wordt de pincode ontfutseld. Daarna wordt het geld snel weg gepind.

Hoe herken ik bankhelpdeskfraude?

- Een bank zal **nooit** naar uw saldo vragen, ook niet als controlevraag.
- Een bank zal u **nooit** vragen om geld over te maken naar een andere, zogenaamde, ‘kluisrekening’ of ‘veilige rekening’. **Zulke rekeningen bestaan niet**.
- Uw bank zal u **nooit** onder druk zetten zo snel mogelijk te handelen. Een bank heeft namelijk zelf de mogelijkheid om een rekening te blokkeren en zal dat ook doen als dat nodig is. Als de bank uw rekening heeft moeten blokkeren, zal de bank u hierover bellen. Vertrouwt u dit niet, hang op en bel zelf de bank op om navraag te doen.
- Komt een leidinggevende van de betreffende organisatie aan de lijn? Let op, dat is ook een oplichter die in het complot zit.

Wat kan ik doen als ik zo’n telefoontje krijg?

- Verbreek direct de verbinding.

- Bel dan zelf uw bank via een algemeen bekend nummer en wacht tot u iemand aan de lijn krijgt. Dan kunt u zelf controleren of datgene wat is verteld wel klopt.
- TIP: Probeer het telefoonnummer, waarmee u gebeld bent, te noteren en door te geven aan de bank/politie.

Wat moet ik doen als ik al slachtoffer ben van bankhelpdeskfraude?

- Doe altijd aangifte bij de politie. Dat kan bijvoorbeeld via nummer 0900 - 8844. Meer informatie over aangifte doen van deze en andere cyberdelicten? Kijk op de website van de politie.
  Kijk op: https://www.politie.nl/aangifte-of-melding-doen#ik-ben-op-een-andere-wijze-opgelicht
- Via uw wijkagent, kijk op: https://www.politie.nl/mijn-buurt/wijkagenten
- Bel ook direct uw bank. Zowel ter voorkoming van (vervolg-)schade als voor het aanvragen van mogelijke compensatie.
- Als u daar behoefte aan heeft, bel dan slachtofferhulp.
  https://www.slachtofferhulp.nl/hulp-bij-jouw-situatie/

Banken informatie punt.

De gezamenlijke banken hebben een website waarop u informatie kunt vinden. U kunt hier informatie vinden over allerlei bankzaken.
Voor meer informatie, kijk op: https://bankinformatiepunt.nl/

Betaallimieten

Tegenwoordig wordt er vaak met de telefoon betaald. Dit is uiteraard erg makkelijk maar let op. De betaallimiet vanuit je *reguliere bankrekening* en die van Google Pay en Apple Pag is vaak anders dan je zelf hebt ingesteld op je eigen bank.
Lees meer over **Google Pay**: https://pay.google.com/intl/nl_be/about/
en **Apple Pay:** https://www.apple.com/nl/apple-pay/

Telefoonnummer spoofing

Bij spoofing met telefoonnummers nemen de oplichters een **ander telefoonnummer** aan. Ze bellen bijvoorbeeld met een Nederlands nummer terwijl zij zich helemaal niet in Nederland bevinden. Deze truc wordt veel gebruikt bij helpdeskfraude, waarbij oplichters u bellen namens een helpdesk van grote bedrijven zoals Microsoft. Uiteindelijk hopen ze u ertoe aan te sporen om de beller de controle over uw computer te geven, zogenaamd om een bepaalde bug (een fout of storing in software of hardware) te verhelpen.

Hoe kunt u zien dat het om een valse e-mail gaat?

- Let altijd op de afzender. Eindigt het e-mailadres van de afzender niet op @naam bedrijf.nl? Dan is de kans groot dat deze mail nep is. Overigens spelen criminelen hier tegenwoordig goed op in. Zo laten ze het afzenderadres eindigen op .com in plaats van .nl of wijkt het adres een lettertje af van het originele e-mailadres. Handige fraudeurs maken gebruik van een trucje dat **'e-mail spoofing'** heet. Hierbij kunnen ze het afzenderadres zo manipuleren dat het niet meer van het origineel is te onderscheiden.
- **Staat er een link in de e-mail?** Check dan eerst waar de link naartoe leidt door met de cursor van uw muis iets boven op de link te gaan staan zonder te klikken. Hiermee kunt u zien naar wat voor website u gaat als u op de link klikt. Komt de URL helemaal niet overeen met de URL van de officiële website van een bedrijf of instantie? Dan is dit een

valse website.
Let wel op: ook de URL's lijken tegenwoordig erg op de URL van een officiële website. Echte URL: www.ing of WWW.ING.NL dit is een valse URL die echt lijkt www.lNG.nl. De l is de kleine letter l (eo)

Zo checkt u een link:

- Bevat de e-mail een bijlage? Klik **nooit** zomaar op deze bijlage. Met slechts een klik kunt u al schadelijke software op uw computer downloaden. Check op dezelfde manier als bij phishing mails, waar de link naar toe gaat, of wat voor bestand u downloadt. (www.checkjelinkje)
  Bijlagen met de extensie .exe of .zip zijn vaak risicovol. **Open deze bijlagen niet** voordat u het e.e.a. gecontroleerd.
- Kijk goed naar de strekking van het bericht. Banken sturen bijvoorbeeld **nooit** e-mails waarin staat dat u uw gegevens moet invullen. Ook vragen ze u **nooit** uw bankpas op te sturen. Wordt er gedreigd met een aanmaning of deurwaarder? Trap er niet in! Dit doen de fraudeurs alleen maar om u bang te maken en u onder druk te zetten. Vaak geeft de e-mail u een valse urgente reden om actie te ondernemen.
- Let op spelfouten en de vormgeving van de e-mail. Ziet de e-mail er amateuristisch uit? Dan kunt u er bijna direct vanuit gaan dat het een valse e-mail betreft. Criminelen worden steeds beter in het kopiëren van een betrouwbare vormgeving door het gebruik van dezelfde kleuren, logo's, lettertype en namen. Laat de vormgeving u niet misleiden.

Malafide handelspartijen.

Op de website van de politie vindt u een lijst met handelspartijen (verkopers en handelaren) die als malafide bekend staan bij de politie. De politie raadt u alle handel met deze partijen af. Op deze pagina vindt u mailadressen, websites (url's) en rekeningnummers van deze handelaren. Voordat u iets koopt, check altijd de gegevens van de verkoper.

Let op!

Aan deze checkfunctie kunt u geen rechten ontlenen. Mogelijk heeft u gelezen dat er geen meldingen zijn tegen de (ver)koper. Of dat de politie (op dit moment) nog geen vermoedens heeft van een strafbaar feit. Toch kunt u nog steeds risico lopen bij een verdere transactie. Blijf dus altijd alert en gebruik uw gezonde verstand. Wanneer iets te mooi is om waar te zijn, dan is dat meestal ook zo!

Dit is de link naar de site https://www.politie.nl/aangifte-of-melding-doen/bekende-malafide-handelspartijen.html

Leuke links:

U kunt op https://checkjelinkje.nl/ uw link altijd controleren.

Voor WhatsApp kunt u https://checkjelinkje.nl/appjelinkje gebruiken.

Weet u nog steeds niet zeker of een e-mail verstuurd is door het bedrijf of instantie waar de e-mail vandaan lijkt te komen? Neem dan contact op via het telefoonnummer of e-mailadres dat op de officiële website van de instantie of het bedrijf te vinden is.

Pas op voor e-mails waarin staat dat u een prijs heeft gewonnen. Vul uw gegevens niet in. Als het te mooi lijkt om waar te zijn, is dat meestal ook zo.

Welke soorten frauduleuze e-mails zijn er en hoe herken ik ze?

Website spoofing (ook wel URL spoofing genoemd).

Website spoofing komt u vaak tegen in combinatie met een **valse e-mail**. Als u op een link van een valse e-mail klikt, kunt u terecht komen op een nepwebsite die precies lijkt op de officiële website. Dit is website spoofing.
Bij website spoofing wordt een website nagemaakt van een bank of een organisatie. De criminelen willen ermee zorgen dat u erin trapt en uw gegevens invult. Vaak lijkt de URL in de adresbalk veel op die van de echte website, maar staan er een aantal letters verkeerd of eindigt het niet op .nl maar op een andere landscode. Dit wordt ook wel 'typosquatting' genoemd.

Advies:

U kunt ervoor zorgen dat u hier niet intrapt door de URL (het internetadres, https://www.naamwebsite.nl) handmatig in te typen in uw browser en deze vervolgens te vergelijken met de URL van de nepwebsite. Als dit niet overeenkomt, heeft u hoogstwaarschijnlijk te maken met een nepwebsite!

SMS-spoofing

U krijgt een SMS of ander tekstbericht van een bekende persoon of organisatie, bijvoorbeeld uw boekhouder. Het nummer en de naam in het bericht kloppen. Uw boekhouder vraagt of u direct een openstaande factuur wilt betalen. In werkelijkheid is het een oplichter die een tekstbericht van uw boekhouder heeft nagemaakt. Zo'n bericht is bijna niet van echt te onderscheiden, maar vaak zal een oplichter benadrukken dat er per direct actie nodig is. Reageer niet op het tekstbericht en klik niet op een link daarin. Neem zelf contact op met uw boekhouder, bijvoorbeeld via de telefoon.

Nummer spoofing

Een bekende lijkt u te bellen, bijvoorbeeld uw eigen bank. Het nummer klopt. Alleen heeft u geen bankmedewerker aan de lijn, maar een crimineel die u probeert op te lichten. Die vraagt u bijvoorbeeld een overboeking te doen of uw pincode te geven. Verwacht u geen telefoontje van uw bank of vertrouwt u het niet? Verbreek de verbinding en bel zelf naar uw bank.

Vriend in Nood (WhatsApp fraude)

Een vriend, familielid of andere bekende stuurt een bericht dat hij **dringend financiële** hulp nodig heeft. De bekende zit bijvoorbeeld zogenaamd in het buitenland vast en is zijn geld, telefoon en papieren kwijt. Of hij heeft zijn telefoon per ongeluk in de wasmachine gedaan en kan daarom niet internetbankieren. Deze 'bekende' vraagt u om snel geld over te maken. Als u hieraan meewerkt, volgt er vaak een tweede verzoek.
Achteraf blijkt het account van deze vriend gehackt te zijn. Het kan ook zijn dat de oplichter een vals account of een nieuw telefoonnummer gebruikte. De echte bekende in kwestie is zich van geen kwaad bewust. Deze vorm van fraude wordt ook wel vriend-in-noodfraude genoemd. Dit komt op WhatsApp verreweg het meeste voor maar kan ook plaatsvinden via e-mail, SMS, Snapchat en Telegram.

TIP:

Neem altijd contact op met degene die u een bericht stuurt. In veel gevallen heeft u het nummer in uw telefoon staan. Bel hem of haar op het bij u bekende nummer.

Maak in ieder geval NOOIT geld over!!!!

Niet gebeld is GEEN geld

Preventiemaatregelen

- Nummer blokkeren WhatsApp.
  Als u het slachtoffer bent geworden van een **Vriend in Nood** WA dan kunt u het nummer waarmee de oplichter/crimineel u heeft benaderd blokkeren.
  Lees meer over blokkeren WhatsApp.
  Type in uw adresbalk:
  https://faq.whatsapp.com/1142481766359885/?locale=nl_NL&cms_platform=iphone
- Schaf een goede virusscanner aan.
  Heeft u per ongeluk toch op een bijlage die malware bevat geklikt? Dan kan de virusscanner in sommige gevallen voorkomen dat uw computer geïnfecteerd wordt.
- Stel uw computer, smartphone of tablet zodanig in dat de updates **ALTIJD** geïnstalleerd worden. Updates van de software zijn belangrijk om te zorgen dat alles veilig blijft.
- Let op als u ergens bent en gebruik kunt maken van 'gratis' internet, denk aan een terras, restaurant of dergelijke. ***Doe dit alleen als het niet anders kan***. De reden is dat u onbeschermd bent voor personen die uw telefoon willen hacken.

Hoe vakantieveilingen je in de val lokken.

De cybercriminelen hebben weer een nieuw gebied gevonden om mensen op te lichten.
U kunt dit bericht plus een bijbehorend filmpje vinden op https://www.ccinfo.nl/menu-hulpmiddelen-kwetsbaarheden/tips/2560435_hoe-vakantieboekingen-je-in-de-val-kunnen-lokken-voorkom-oplichting-met-deze-tips

Wat is malware?

'Malware' is software die specifiek is ontwikkeld om schade toe te brengen aan een computer. Malware kan gevoelige informatie van uw computer stelen, uw computer geleidelijk vertragen en zelfs nepmails versturen vanuit uw e-mailaccount zonder uw medeweten.

Overname besturing computer

Criminelen proberen op allerlei manier achter wachtwoorden en gebruikersnamen te komen met als doel in te kunnen loggen.

Het kan voorkomen dat ze zogenaamd van een organisatie (uw bank / Microsoft o.i.d.) u benaderen dat er een probleem is met uw bankrekening, tijdens de betaling is er iets fout gegaan waardoor de betaling of een overboeking niet is geslaagd.
Normaliter zou men langskomen maar het is ook mogelijk dat ze een bestandje naar u sturen, dan moet u installeren dan kan de beller op afstand uw computer 'overnemen' en uw probleem oplossen. **Accepteer dat nooit**! Het is een methode die vandaag de dag ook nog werkt. Denk hierbij aan bankhelpdesk fraude of andere manieren om achter uw gegevens te komen.
Beruchte programma's zijn onder andere:
Anydesk
Anywhere
Maar er zijn er uiteraard meer. Installeer NOOIT op verzoek van een ander/onbekende zo'n programma. Ze wijzigen uw wachtwoorden en u kunt niet meer werken met uw eigen apparaat (i.p.v. device).
Meldt het ALTIJD bij de politie.

Sterke wachtwoorden

Om het criminelen lastig te maken is het belangrijk dat u 'sterke' wachtwoorden gebruikt.
Er zijn meerdere mogelijkheden om hier goed mee om te gaan.
https://www.seniorweb.nl/artikel/omgaan-met-wachtwoorden
Voorbeelden:
Tijdens de presentatie is er een filmpje getoond waarbij werd gesproken over een **wachtwoord zin**. Als voorbeeld werd een eenvoudige zin gebruikt als wachtwoord.
TIP: Maak ook door middel van een eenvoudige, makkelijk te onthouden, zin een wachtwoord.
Enkele voorbeelden:

- Ik heb een grijze Gazelle elektrische herenfiets
- Mijn eerste auto was een Renault

Voor het kraken van deze twee 'eenvoudige' wachtwoordzinnen heeft een hacker meer dan 1000 jaar nodig. Als er nog gekozen wordt om er cijfers in te verwerken en leestekens dan duurt het nog veel langer.
Kijk voor meer info dit filmpje op Youtube:
https://www.youtube.com/watch?v=6n-ZoFW-d_I
Sterke wachtwoorden maken, onthouden en veilig opslaan.
Hieronder vindt u enkele tips om veilig om te gaan met wachtwoorden:
https://www.seniorweb.nl/tip/automatisch-wachtwoorden-invullen-op-iphone-ipad
https://www.seniorweb.nl/artikel/wachtwoorden-betaalmethoden-en-adressen-bewaren-in-edge
Wachtwoorden manager: https://www.seniorweb.nl/artikel/wachtwoordmanager-bitwarden
Wachtwoorden manager: https://www.seniorweb.nl/artikel/lastpass-gebruiken
Chrome: https://www.seniorweb.nl/tip/geen-wachtwoorden-opslaan-in-chrome
Wachtwoorden check: https://passwords.google.com/intro
https://www.seniorweb.nl/tip/chrome-sterke-wachtwoorden-laten-bedenken
https://www.seniorweb.nl/tip/een-veilig-wachtwoord-maken-en-onthouden
Wachtwoordkraaktest
https://veiliginternetten.nl/wachtwoordkraaktest/

Wachtwoorden generator en kluis.

Momenteel werkt Blue Professionals samen met **Senioren Brabant Zeeland en Seniorweb** aan ontwikkelen van een wachtwoorden generator en een kluis.
Dit wordt samen gedaan met het bedrijf MindYourPass een ***Nederlands*** bedrijf dat is gevestigd op de High Tech Campus in Eindhoven.
Voordeel is dat het een **Nederlands bedrijf** is dat gegevens slim bewaard.
Bovendien is het geheel voor **particulieren** gratis

ORGANISATIES:
Er is ook een versie voor organisaties die wel betaald moet worden. Steeds meer organisaties (gemeenten/bibliotheek etc) kiezen voor een Nederlandse organisatie en niet meer voor Amerikaanse bedrijven. Hierdoor kan men https://mindyourpass.io/nl gratis aanbieden aan particulieren.

Twee-staps-verificatie

Er zijn tegenwoordig ook extra mogelijkheden om het hacken moeilijker te maken door gebruik te maken van **twee-staps-verificatie.**

(https://veiliginternetten.nl/thema/basisbeveiliging/wat-tweestapsverificatie/) voor meer informatie of op de site van de Consumentenbond. https://www.consumentenbond.nl/veilig-internetten/activeer-tweestaps-authenticatie) waar u trouwens nog veel meer informatie kunt vinden over veilig internetten.

Maar ook op de website van Seniorweb staat de informatie.
type https://www.seniorweb.nl/tip/wat-is-tweestapsverificatie

Nieuwe ontwikkelingen.

Een van de belangrijkste ontwikkelingen is **Kunstmatige intelligentie**.
Kunstmatige intelligentie of Artificiële Intelligentie (afgekort AI) maakt al een langere tijd deel uit van ons dagelijks leven. Nu al gebruiken we de gezichtsherkenning in onze smartphones, antwoorden van chatbots en de film- en muziekaanbevelingen op basis van eerdere beoordelingen. Maar de toekomst belooft ons meer. AI moet gaan zorgen voor snelle en juiste medische diagnoses, zelfrijdende auto's, robots die hun 'zintuigen' gebruiken en nog veel meer.
Welke zijn er inmiddels?

- ChatGPT (Open AI
- Copilot (Microsoft)

- Gemini (Google)
- Etc

Op internet kunt u nog veel meer ontdekken
Lees meer over AI:
https://www.rdi.nl/onderwerpen/kunstmatige-intelligentie/wat-is-kunstmatige-intelligentie
Chatbot:
In de media verschijnen de laatste tijd allerlei berichten over Kunstmatige Intelligentie (Artificial Intelligence AI). Dit zijn wel ontwikkelingen die veel invloed kunnen hebben. Ongetwijfeld heeft u op een website wel eens een column gezien waarin u uw vraag kunt stellen aan ……..
Dit is een zogenaamde chatbot die ontwikkeld is en antwoord kan geven op uw vraag.
Het zijn vaak "zelflerende" programma's die – inderdaad – met behulp van AI worden ontwikkeld.
Voice cloning
Bij het klonen van stemmen wordt gebruik gemaakt van kunstmatige-intelligentietechnieken om een machinaal lerend stemmodel te trainen op de echte opnames om spectrums van de stem te extraheren en een stem te creëren die bijna precies klinkt als de echte stem.
Dit is een ontwikkeling die 'gevaarlijk' kan zijn. U heeft het idee dat er een bekende belt maar dat blijkt dus een computerstem te zijn.
Denk aan het filmpje waarbij Oma gebeld wordt door haar zogenaamde kleindichter "Joy", maar wat in werkelijkheid een ma was.
ChatGPT
ChatGPT is een chatbot op basis van kunstmatige intelligentie (KI of AI). De tool werkt zoals iedere andere chatbot. Gebruikers typen teksten in de vorm van prompts (een prompt is een korte tekst die je gebruikt om een AI-tool te laten reageren) en de tool antwoordt met een eigen tekst. Wat ChatGPT zo uniek maakt is hoe vloeiend, uitgebreid en menselijk klinkend de antwoorden zijn, evenals het grote aantal onderwerpen dat de tool kan bespreken.
Door AI gegenereerde foto's
De ontwikkelingen van AI volgen elkaar razendsnel op, maar er komen steeds vaker signalen van minder positieve ontwikkelingen. Zo werden in een dorp in Spanje foto's van meiden tussen 11 en 17 jaar zodanig bewerkt dat er naaktfoto's werden gepresenteerd.
Sora AI heeft een programma ontwikkeld waarbij je de meest fantastische beelden/filmpjes kunt maken. Kijk op: https://www.youtube.com/watch?v=TU1gMloI0kc De moeite waard

Cash en card Trapping

Wat is cash en card trapping?
Bij **cash trapping** manipuleren dieven de geldautomaat zodat er geen geld uit de machine komt. Ze plaatsen een afdekplaatje voor de gleuf van de geldautomaat. De geldautomaat doorloopt de hele (gelduitgifte)procedure. *Op het scherm ziet u dus 'neem pas uit' of 'geld uitnemen', maar het geld komt niet uit de automaat*. U denkt waarschijnlijk dat de automaat defect is.
Als de bank open is, loopt u misschien naar binnen om het bankpersoneel te waarschuwen.
Als de bank gesloten is, of de geldautomaat staat niet in de buurt van een bank, dan loopt u waarschijnlijk weg. Zodra u de bank binnenloopt of de hoek om bent, halen de cash trappers het geld uit de geldautomaat en gaan zij er met uw geld vandoor.
Wat kan ik doen en wat moet ik doen?

U kunt niets doen om cash trapping te voorkomen, maar u kunt wel voorkomen dat cash trappers er met uw geld vandoor gaan. Krijgt u geen geld na een geldopname bij de automaat? Het telefoonnummer van de bank staat op de geldautomaat en u vindt de meldnummers online. Blijf bij de automaat staan, terwijl u belt. Dan kunnen de criminelen niet bij uw geld.

Soorten fraude:

Dating- én beleggingsfraude: wat is 'pig butchering'?

Steeds meer mensen vallen voor een oplichtingspraktijk die bekendstaat als 'pig butchering'. Maar wat houdt deze vorm van fraude precies in?

Datingfraude is één van de fraudes die momenteel het snelst stijgt.

Kijk hier voor meer informatie:

https://panorama.nl/artikel/623723/dating-en-beleggingsfraude-wat-is-pig-butchering

En lees hier het verhaal van Mathijs https://www.nu.nl/economie/6336012/online-criminelen-slaan-slag-op-datingsites-het-geld-is-in-een-klap-weg.html

https://slachtofferwijzer.nl/artikelen/wat-is-pig-butchering

https://hetccv.nl/themas/high-impact-crimes/datingfraude/

Boilerroomfraude

is een vorm van beleggingsfraude waarbij criminelen ongevraagd contact opnemen (meestal telefonisch) met een veelbelovend beleggingsaanbod. Ze lokken slachtoffers met een eerste, winstgevende investering om ze vervolgens onder druk te zetten om steeds grotere bedragen te storten in nep-aandelen of waardeloze producten. Het geld is daarna vaak voorgoed kwijt.

Kenmerken van boilerroomfraude

- **Ongevraagde benadering:** Oplichters nemen vaak telefonisch contact op, zonder dat u erom heeft gevraagd.
- **Veelbelovende aanbiedingen:** Ze presenteren een fantastische deal met hoge verwachte rendementen.
- **Druk:** Ze zetten u onder druk om steeds meer geld te investeren, soms zelfs na een succesvolle eerste investering.
- **Professionele uitstraling:** Oplichters doen zich voor als legitieme dienstverleners, met professioneel ogende websites en formulieren.
- **Verliesgevende investeringen:** Uiteindelijk blijken de investeringen waardeloos te zijn of het geld verdwijnt en kunt u het niet terugkrijgen.
- **Hersteloplichting:** Soms nemen frauduleuze 'recovery' bedrijven contact op om zogenaamd het verloren geld terug te halen, waarvoor u weer moet betalen. Dit is vaak een nieuwe vorm van oplichting.

Wat kunt of moet u doen als u slachtoffer bent?

- **Doe aangifte:** Neem contact op met de politie via 0900-8844. Verzamel zoveel mogelijk benodigde gegevens voordat u belt.
- **Meld bij de AFM:** Meld de mogelijke fraude bij de Autoriteit Financiële Markten (AFM). Dit kan helpen bij hun onderzoek.
- **Zoek juridisch advies:** Het is verstandig om juridisch advies in te winnen. Het Juridisch Loket kan hierbij helpen. Klik voor meer informatie op https://www.juridischloket.nl/
- Neem voor ondersteuning en advies contact op met https://www.slachtofferhulp.nl/hulp-bij-jouw-situatie/
- Doe **ALTIJD aangifte** bij de politie en meldt het bij de Fraudehelpdesk: https://www.fraudehelpdesk.nl/

QR-Code

Steeds vaker zie je QR-codes voorbijkomen in het dagelijks leven. Zo scan je het menu in een restaurant, staat je handleidingen in een QR-code of betaal je een tikkie gemakkelijk door het scannen van een QR-code. Waar het gebruiksgemak van QR-codes steeds meer toeneemt zien wij ook een stijging in deze vorm van cybercrime.
https://www.surelock.nl/waarom-een-qr-code-zo-gevaarlijk-is/
Politie waarschuwt ook voor valse QR-codes bijvoorbeeld bij een parkeerautomaat:
https://www.rtl.nl/nieuws/artikel/5481316/valse-qr-codes-op-parkeerautomaten
Hieronder ziet u een veilig QR. Probeer het maar eens uit.
Iedereen kan dus gratis een QR code maken, ook de criminelen.
Leuk filmpje over QR codes en nog meer leuke tips:
https://geldland.nl/ontdek-wat-je-kunt-doen-met-qr-codes/

Dit is een QR die je zelf kunt maken. Kijk op:
https://me-qr.com/nl/qr-code-generator/qr
Links is een veilige QR. Door deze te scannen komt u uit op de website van www.blue-professionals.nl

Quishing

Criminele proberen d.m.v. een QR-code een phising bericht te verzenden. Vaak scherpe aanbiedingen.

Meer info over deze toenemende manier van Phishing kunt u vinden op
https://insights.centric.eu/nl/themes/cybersecurity/pas-op-voor-quishing-zijn-qr-codes-nog-veilig-te-gebruiken/
Filmpje van geldland >>> https://geldland.nl/ontdek-wat-je-kunt-doen-met-qr-codes/

Fraude met cadeaukaarten.

Frauderen met cadeaukaarten is populair onder kwaadwillenden. Een aantal tips als u een cadeaukaart wilt aanschaffen of u heeft er een ontvangen.

1. Wanneer je online cadeaukaarten koopt, bestel deze dan rechtstreeks bij een detailhandelaar en niet bij buitenlandse onbekende online winkels.
2. Koop alleen cadeaukaarten die beschikken over een pincode.
3. Als een aanbieding te mooi lijkt om waar te zijn, dan is dat het meestal ook.
4. Wees je ervan bewust dat geen enkel bedrijf of overheidsfunctionaris zal vragen om een betaling met cadeaubonnen.
5. Geef nooit persoonlijke en financiële gegevens op na ongevraagd contact online.
6. Laat het tegoed van de cadeaukaart niet te lang op de kaart staan. Des te langer de cadeaukaart bewaard wordt, des te groter de kans is dat gegevens gekraakt worden of worden misbruikt.
7. Controleer het kaartsaldo zodra je de kaart krijgt.

Leuke link met verklaring afkortingen en digi woorden.

In de digitale wereld komt u afkortingen of woorden tegen die nog niet zo bekend zijn.
ESET heeft voor de meeste woorden of afkortingen een mooie omschrijven geschreven.

Kijk voor meer informatie op https://onlineveilig.eset.com/woordenboek/

Fraude Booking.com

Steeds meer gedupeerde reizigers maken melding van online fraude via het populaire boekingsplatform Booking.com, meldt het AD. Heb jij een accommodatie geboekt via Booking.com? Dit is waar je op moet letten.

Lees meer op https://opgelicht.avrotros.nl/nieuws/artikel/fraude-via-bookingcom-neemt-toe-gemiddelde-schade-van-854-euro-per-persoon/

Advies

Heeft u geboekt via Booking.com? Wees dan alert op berichten die mogelijk van kwaadwillende afkomstig zijn. Krijgt u een verificatieverzoek of een ander bericht waarin om gegevens of geld wordt gevraagd? ***Neem dan contact op met Booking.com of met de accommodatie waar u geboekt heeft. Controleer of het ontvangen bericht betrouwbaar is of dat u mogelijk met oplichters te maken heeft.***

Digitaal 'testament'.

Als je actief bent op de diverse sociale netwerken is het goed om eens na te denken op welke wijze u het opzeggen van uw accounts regelt, als u komt te overlijden of u bent niet meer in staat om zelfstandig handelingen te verrichten.

Een optie is één van de kinderen aan te wijzen (in goed overleg) en deze alles verder laten afhandelen.

Een belangrijk onderwerp waar wel wat vaker over gesproken mag worden.

Meer informatie en hoe je dit eventueel kunt regelen kunt u lezen op https://veiliginternetten.nl/digitale-nalatenschap/

Wanneer belt u 0900 – 8844 en wanneer 112?

U belt alleen 112 bij **spoedeisende** zaken.

Bijvoorbeeld bij:

- levensbedreigende situaties
- als u een misdrijf ziet
- verdachte situaties
- u heeft toch met die 'bankmedewerker' een afspraak gemaakt.

Voor alles wat 'zonder zwaailicht' kan en voor informatie en advies kiest u 0900-8844.

Kifid waarschuwt voor koopkrediet.

Kifid waarschuwt mensen om niet in zee te gaan met KoopKrediet. Meer informatie kunt u vinden op: Kifid waarschuwt voor KoopKrediet (https://www.kifid.nl/nieuws/kifid-waarschuwt-voor-koopkrediet/)

Leuke nieuwe link (veilig)

Online criminelen doen zich vaak voor als een bekende... in dit geval ben jij die bekende. Nu kan je zelf een phishing berichtje sturen aan iemand die je kent. Zo ontdek je wat de technieken zijn. En dan: *even afwachten… laat die ander zich* ***interneppen?***
Lees meer op:
www.phishkraam.nl

Via deze site kunt u een onschuldig nepbericht verzenden. Online criminelen doen zich vaak voor als een bekende... in dit geval ben jij die bekende.

Om even over na te denken:

Lees deze stellingen eens rustig door en geef dan een eerlijk antwoord op die stellingen.
U zult ontdekken dat sommige zaken iets verbeterd kunnen worden. Veel succes.

- Ik maak regelmatig back-ups van belangrijke bestanden die op mijn laptop staan.
- Ik klik zelden of nooit op een bijlage of link in een mail waarvan ik de afzender niet ken.
- Ik post op sociale media zelden persoonlijke informatie zoals mijn verjaardag of een nieuwe aankoop.
- Ik heb een virusscanner op mijn laptop.
- Mijn wachtwoorden zijn moeilijk te herleiden.
- Ik verander mijn wachtwoorden regelmatig.
- Ik draai regelmatig updates op mijn laptop en/of telefoon.
- Mijn laptop is vergrendeld (met bv. een wachtwoord).
- Ik open nooit een linkje in de mails die ik van mijn bank krijg.
- Ik neem nooit onbekende telefoonnummers op.
- Ik gebruik nooit openbare (niet-beveiligde) wifinetwerken.
- Ik log altijd uit nadat ik een site heb bezocht waarvoor ik moest inloggen, zoals mijn e-mail of een webwinkel

Stappenplan voor meer veiligheid

- Voer regelmatig updates uit (check de legitimiteit/Playstore/Apple store).
- Installeer een antivirusprogramma zoals Norton of McAfee als je geen antivirussoftware hebt via Microsoft 11 of Apple.
- Vergrendel je telefoon en je laptop (met een wachtwoord, een vingerafdruk of een pincode/patroon).
- Bescherm je gegevens: maak regelmatig back-ups, ook als je in de Cloud werkt.
- Gebruik sterke wachtwoorden of wachtzinnen (+ passwordmanager zoals Lastpass) kijk op: https://www.lastpass.com/nl
- Werk altijd via een veilige verbinding: kijk uit met gratis, openbare wifi. Verbinding (niet wifi) van je provider is dan waarschijnlijk veiliger.
- Multifactor-authentificatie voor met name financiële en medische sites. Kijk voor meer informatie op https://veiliginternetten.nl/wat-tweestapsverificatie/
- Check links door er met je muis op te gaan staan (er boven ‘hangen’, niet klikken).

- Deel niet te veel op sociale media, zeker geen afwezigheid, vakanties, grote aankopen. Kijk uit met foto's van (klein-)kinderen en die van uzelf.
- Blijf alert en voorzichtig, gebruik je gezonde verstand.
- Vraag anderen om hulp als je iets niet vertrouwt!

Odido hack

- Inlognaam en wachtwoord
- Volledige naam
- Woonadres
- Telefoonnummer
- E-mailadres
- IBAN-nummer
- En aanvullende klantgegevens, bekend bij Odido

Hoe bescherm je jezelf tegen identiteitsdiefstal?

Voordat je slachtoffer kunt worden van identiteitsdiefstal, moeten criminelen eerst je persoonlijke gegevens stelen, zoals je naam, telefoonnummer, geboortedatum, Burgerservicenummer, adres en creditcardnummer. De belangrijkste manier waarop ze dit doen, is door toegang te krijgen tot online accounts met een slechte beveiliging. Daarom is het beveiligen van je accounts belangrijker dan ooit. Door de onderstaande eenvoudige stappen te volgen, kun je je persoonlijke gegevens beschermen en het risico op identiteitsdiefstal aanzienlijk verkleinen:

Meer info: https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/identiteitsfraude-voorkomen

- Voeg uw e-mailadres toe aan de 24/7-inbreukbewaking in uw beveiligingsapp;
- Gebruik unieke wachtwoorden (gegenereerd met een sterke wachtwoordgenerator https://www.f-secure.com/en/password-generator)
- 2FA gebruiken https://www.seniorweb.nl/artikel/wat-is-tweestapsverificatie
- Gebruik antivirussoftware die bank- en winkelactiviteiten controleert;
- Wees voorzichtig bij het openen van links en bijlagen. Gebruik www.checkjelinkje.nl ;
- Gebruik een **VPN** op openbare wifi-netwerken. Kijk voor meer informatie op https://www.consumentenbond.nl/veilig-internetten/beste-vpn-aanbieder
- **Een VPN** (Virtual Private Network) is een beveiligde en versleutelde verbinding tussen jouw apparaat en het internet. Het maskeert je IP-adres en beschermt je data, waardoor je veiliger bent op openbare wifi en anoniemer surft.
  Veiligheid op openbare wifi: Het voorkomt dat hackers op onbeveiligde netwerken (zoals in cafés of hotels) je gegevens kunnen inzien.
- **Privacy:** Je browsegeschiedenis, identiteit en locatie worden verborgen voor pottenkijkers en advertentie trackers.
- **Geografische vrijheid:** Door een server in een ander land te kiezen, omzeil je soms geografische restricties voor content of diensten

10 tekenen van identiteitsdiefstal

Hoewel het beschermen van uw online accounts de meest effectieve manier is om identiteitsdiefstal te voorkomen, is het ook belangrijk om op de hoogte te zijn van de belangrijkste waarschuwingssignalen. Deze signalen helpen u te weten waar u op moet letten en stellen u in staat snel te reageren, zodat de schade tot een minimum wordt beperkt.
Belangrijke factoren om rekening mee te houden zijn onder andere:

- Uw persoonlijke gegevens die openbaar worden gemaakt bij een datalek;
- Als je een uitkering aanvraagt, krijg je te horen dat je die al ontvangt;
- Nieuwe rekeningen die in uw kredietrapport verschijnen;
- Het opsporen van malware die op een van uw apparaten is geïnstalleerd;
- Het opsporen van uitgaande betalingen voor goederen en diensten die u niet hebt gedaan;
- Onverwachte telefoontjes of bezoekjes van incassobureaus ontvangen;
- Een plotselinge daling van uw kredietscore zien;
- Krediet geweigerd krijgen zonder eerdere problemen;
- Merken dat er geen financiële documenten meer bij u thuis aankomen;
- Een telefoontje van uw bank ontvangen waarin u wordt geïnformeerd over verdachte betalingen.

Wero komt er aan.

Ideal wordt in de loop van 2026 – 2027 vervangen door Wero.
Kijk voor meer informatie op https://ideal.nl/naar-wero
https://www.rabobank.nl/bedrijven/betalen/zelf-betalingen-doen/van-ideal-naar-wero

Belastingdienst

De belastingdienst heeft per 1 mei 2026 een ander bankrekeningnummer. De belastingdienst moet periodiek kijken welke bank het “goedkoopst” is. Nu gaat men bankieren bij de RABO bank.
Dit gebeurt automatisch!!!
Reageer niet op Phishing mails die u vragen om uw gegevens te controleren. Dit gaat – net als bij WERO – automatisch.
Lees meer >>> https://www.belastingdienst.nl/wps/wcm/connect/nl/nieuwe-huisbank/nieuwe-bank-belastingdienst

6 maanden gratis lid van Seniorweb.

U heeft nu de mogelijkheid om gratis 6 maanden lid te worden van Seniorweb. Meer informatie en voorwaarden vindt u hier, https://www.seniorweb.nl/senioren

Maken van een back-up.

Een back-up maken beschermt je gegevens tegen verlies. Gebruik een externe harde schijf, USB-stick of clouddiensten (Google Drive, OneDrive, iCloud) voor automatische opslag. Belangrijke bestanden, foto's en instellingen kun je ook handmatig via apparaat instellingen veiligstellen.

Back-up maken op Windows (10/11)

Dit kan op de onderstaande manieren:

- Bestandsgeschiedenis (Externe Schijf): Ga naar Instellingen > Bijwerken en beveiliging > Back-up (of Configuratiescherm > Bestandsgeschiedenis) en voeg een station toe om automatisch bestanden op te slaan.
- Microsoft OneDrive (Cloud): Ga naar Instellingen > Accounts > Windows-back-up om mappen (Documenten, Afbeeldingen) direct naar de cloud te synchroniseren.
- Handmatig: Kopieer bestanden direct naar een externe harde schijf of USB-stick.

Back-up maken op Mac (macOS)

- Time Machine (Aanbevolen): Sluit een externe harde schijf aan. Als het goed is, vraagt macOS direct of je deze schijf wilt gebruiken voor Time Machine. Zo niet, ga naar Systeeminstellingen > Algemeen > Time Machine en kies de schijf.
- iCloud Drive: Ga naar Systeeminstellingen > [Uw Naam] > iCloud om documenten en bureaublad direct in de cloud op te slaan.

Belangrijke Tips

Frequentie: Stel automatische back-ups in zodat u er niet aan hoeft te denken.
Locatie: Bewaar ten minste één back-up fysiek los van de computer (op een andere locatie) om schade door brand of diefstal te voorkomen.
Cloud vs. Schijf: Een externe schijf is snel en eenmalig, cloudopslag (OneDrive, iCloud) biedt beveiliging tegen lokale calamiteiten. Er zijn meerdere aanbieders van “cloudruimte”.
Seniorweb.

Op de website van https://www.seniorweb.nl/artikel/een-back-up-van-elk-apparaat kunt u meer informatie vinden. (Aanrader)

Belangrijke en veilige sites:

https://www.fraudehelpdesk.nl/
https://veiliginternetten.nl/
https://www.seniorweb.nl/
https://www.veiligbankieren.nl/
https://www.maakhetzeniettemakkelijk.nl/
https://www.politie.nl/
https://www.digitaltrustcenter.nl/ (heldere informatie, ook voor bedrijven)
https://www.politie.nl/mijn-buurt/wijkagenten (wie is mijn wijkagent?)
https://haveibeenpwned.com/ (controleren of uw gebruikersnaam ooit is ‘misbruikt’. (Datalekken)
https://www.f-secure.com/nl/identity-theft-checker Controleren gegevens nav datalekken)
https://www.f-secure.com/nl/online-shopping-checker Controleren veilige site om te shoppen
https://www.digid.nl/
https://www.rabobank.nl/
https://www.ing.nl/
https://www.abnamro.nl/nl
https://www.regiobank.nl/ (nu https://www.asnbank.nl/home.html)
https://www.snsbank.nl/ (nu https://www.asnbank.nl/home.html)

https://www.asnbank.nl/home.html
https://bankinformatiepunt.nl/
https://opgelicht.avrotros.nl/tag/phishing/
https://opgelicht.avrotros.nl/tag/internetoplichting/
https://geldland.nl/ (leuke tips, onder andere over QR code scannen)
https://www.steffie.nl/eenvoudige-websites/#Geld (mooie informatie over betalen/digid.)
https://bankinformatiepunt.nl/
https://www.digihandig.nl/ (Eenvoudig leren met je smartphone)

Controleren of een site staat geregistreerd.

U kunt altijd controleren of een webshop bekend is bij de politie. De politie houdt dit bij op een lijst, Als er ooit aangifte is gedaan komt de webshop op de lijst te staan.
Kijk hier voor de geregistreerde frauduleuze webshops:
https://www.politie.nl/aangifte-of-melding-doen/bekende-malafide-handelspartijen.html

Nog vragen, opmerkingen of goede tips?

Als er nog vragen of opmerkingen zijn, dan kunt u altijd een e-mailtje sturen naar:
maarten@blue-professionals.nl of info@blue-professionals.nl
We doen ons uiterste best om zo spoedig mogelijk te reageren op uw bericht.
Als u het naslagwerk per e-mail wenst te ontvangen, stuur dan gewoon een mailtje en wij zorgen dat u dit zo snel mogelijk via e-mail ontvangt.
Met vriendelijke groet en maak er een mooie dag van.
Maarten Keijzer
Telefoon: 06 – 21879080
www.blue-professionals.nl

Verzoek:

Als u onderwerpen mis, stuur mij dan een mailtje met uw opmerking. Dan kan ik het verder uitwerken zodat het materiaal steeds completer wordt.

U kunt mij volgen op LinkedIn.

Hier plaats ik met enige regelmaat berichten die over dit onderwerp gaan, of ik stuur relevante berichten door.
Als u mij wilt volgen dan zou ik dat waarderen en dan volg ik u ook.
https://www.linkedin.com/in/8222mk/