Informatie n.a.v. bijeenkomst “Digitale Weerbaarheid Senioren”

Dit naslagwerk is ontwikkeld n.a.v. de bijeenkomsten “Digitale Weerbaarheid Senioren” in de Huiskamers van Overbetuwe. Hieraan hebben meegewerkt:

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 80 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. 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 de hulp 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.

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 (Albert Heijn, Jan Linders, Jumbo, Primera, Gamma).
Als u geld moet pinnen, doe dit dan zoveel mogelijk in een winkel. Daar is veelal publiek 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!

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 fouten, maar dat gebeurt steeds minder.

Phishing is een vorm van cybercrime waarbij criminelen een e-mail 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.

Belangrijk:

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

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. Kijk hier voor meer informatie op het slotje op de adres balk.
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. Klik hier om naar de website te gaan van de fraudehelpdesk. https://www.fraudehelpdesk.nl/ en u kunt deze ook doorsturen naar uw bank

Quizzen:

U kunt door middel van een leuke quiz kijken of u voldoende kennis heeft van **phishing**.

Ga naar de quiz (dit is een veilige website) of type

https://veiliginternetten.nl/thema/cybercrime-en-incidenten/phishing-corona/wat-een-phishingmail/

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

Klik hier. (https://veiliginternetten.nl/quiztool/alert-online-echt-nep-quiz/)
U moet de afbeelding vergroten en op alles letten. Succes.

Spoofing

Spoofing is een truc waarbij een oplichter zich voordoet als een medewerker van uw bank, een helpdesk of webwinkel. Als u geld overmaakt, komt dat terecht bij de oplichter.

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 als dat nodig is.
- 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. Klik hier om naar de site te gaan of type https://www.politie.nl/aangifte-of-melding-doen#ik-ben-op-een-andere-wijze-opgelicht
- Via uw wijkagent. 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.

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 te verhelpen.

Oplichting – bankfraude. Klik hier om het filmpje te bekijken.
Of type over: **https://www.youtube.com/watch?v=DptS7DVz_90&t=101s**

Hoe kunt u zien dat het om een valse 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 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.

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.
  Bijlagen met de extensie .exe of .zip zijn vaak risicovol. Open deze bijlagen niet.
- 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. 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 betrouwbare vormgeving, laat de vormgeving u niet misleiden.

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 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 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.

Nummerspoofing

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

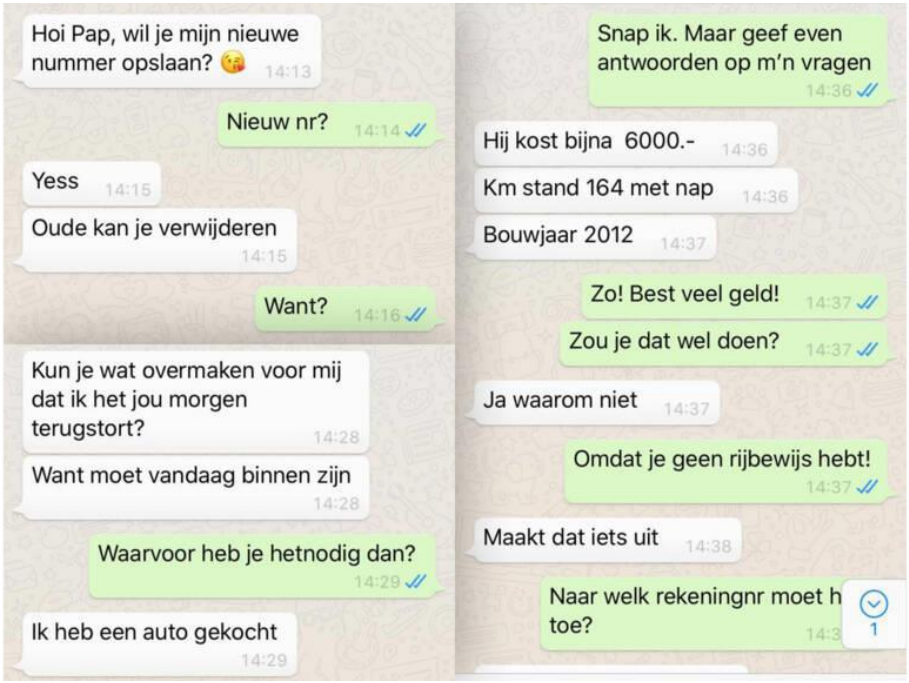
Een vriend, familielid of andere bekende stuurt een bericht dat hij **dringend financiële** hulp nodig heeft. De bekende zit bijvoorbeeld zogenaamd in het buitenland vast en is zijn geld, telefoon en papieren kwijt. Of hij heeft zijn telefoon per ongeluk in de wasmachine gedaan en kan daarom niet internetbankieren. 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.

<u>Maak in ieder geval NOOIT geld over!!!!</u>



Preventiemaatregelen

- Nummer blokkeren WhatsApp.
  Als u het slachtoffer bent geworden van een **Vriend in Nood** dan kunt u het nummer waarmee de oplichter/crimineel u heeft benaderd blokkeren.
  Lees meer over blokkeren WhatsApp. Klik hier >>>> Of 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.

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.

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. Klik hier (of type https://www.seniorweb.nl/artikel/omgaan-met-wachtwoorden) voor meer info van Seniorenweb (https://www.seniorweb.nl/)

Lees meer over de **wachtwoordkraaktest**. Klik hier >>>

https://veiliginternetten.nl/wachtwoordkraak-test/

Voorbeelden:

Tijdens de presentatie is er een filmpje getoond waarbij werd gesproken of 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 nog gekozen wordt om er cijfers in te verwerken en leestekens dan duurt het nog veel langer.

- 15 karakters: alleen kleine letters ➔ 500 jaar
- 15 karakters: kleine en hoofdletters ➔ 17 miljoen jaar
- 15 karakters: kleine- en hoofdletters en cijfers (0-9) ➔ 244 miljoen jaar
- 15 karakters: kleine- en hoofdletters en cijfers (0-9) en speciale tekens ➔ 6 miljard jaar

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

Twee-staps-verificatie

Er zijn tegenwoordig ook extra mogelijkheden om het hacken moeilijker te maken door gebruik te maken van **twee-staps-verificatie.** Klik hier >>> (https://veiliginternetten.nl/thema/basisbeveiliging/wat-tweestapsverificatie/) voor meer informatie of op de site van de Consumentenbond. Klik hier voor 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 Seniorenweb staat de informatie. Klik hier >>> om naar de website van Seniorenweb te gaan of type https://www.seniorweb.nl/tip/wat-is-tweestapsverificatie

Informatie:

De meeste informatie kunt u terugvinden op onze website https://www.blue-professionals.nl/voorlichtingsbijeenkomsten-senioren/

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.politie.nl/mijn-buurt/wijkagenten (wie is mijn wijkagent?)

https://haveibeenpwned.com/ (website om te controleren of uw gebruikersnaam ooit is 'misbruikt'.

https://www.digid.nl/

https://www.rabobank.nl/

https://www.ing.nl/

https://www.abnamro.nl/nl

https://www.regiobank.nl/

https://www.snsbank.nl/

Recente informatie

De politie is actief bezig met het opsporen van frauduleuze website.

Recent is er weer een internationaal opererende site 'opgerold'. Deze hadden van miljoenen mensen hun digitale gegevens ontfutseld waarmee ze van alles konden doen.

Controleren

De politie heeft een website om te controleren of ook uw mailadres is 'gestolen'. U kunt dit controleren op www.checkjehack.nl

U voert uw mailadres in en als u GEEN reactie krijgt is er niets aan de hand. Krijgt u wel een bericht dan moet u zorgen dat u uw wachtwoorden aanpast.

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.

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.

Met vriendelijke groet en maak er een mooie dag van.

Maarten Keijzer

Blue Professionals
Telefoon: 06 – 21879080
www.blue-professionals.nl