ALV 2024 BPV ‘de Ploeg’

INFORMATIE OVER DIGITALE WEERBAARHEID EN VEILIGHEID

Wijkagenten Laren: Remco Wessels en Michelle Kamerbeek

2024

DEEL 2

EEN BIJLAGE CONTROLEREN

Bevat een (verdachte) e-mail een bijlage?

- Klik **nooit** zomaar op deze bijlage. Met één klik kunt u al schadelijke software op uw computer downloaden. Check vooraf net als bij phishing mails, waar de link naar toe gaat. Gebruik de cursor 
- Bijlagen met de extensie **.exe** of **.zip** zijn vaak **risicovol**.
- Kijk naar de strekking van het bericht. Banken sturen nooit e-mails waarin staat dat u uw gegevens moet invullen. Ze vragen nooit uw bankpas op te sturen.
- Negeer dreigingen met een aanmaning, deurwaarder en het CJIB!

EEN LINK CONTROLEREN

Bevat een (verdachte) e-mail een bijlage?

- Let op spelfouten en de vormgeving van de e-mail. Ziet de e-mail er amateuristisch uit? Wel een betrouwbare vormgeving? Laat de vormgeving u niet misleiden. De link controleren kan ook via:

  https://checkjelinkje.nl/ voor email

  https://checkjelinkje.nl/appjelinkje voor WhatsApp

  In mails van **mijn overheid** staat dat u moet inloggen op mijn overheid zonder een link bij te voegen. Dan weet u nagenoeg zeker dat het goed is.

FRAUDULEUZE SMS - WHATSAPP

Soorten en het herkennen

- **SMS - WhatsApp spoofing**
  Bijvoorbeeld een ontvangen SMS of ander tekstbericht van een u bekende persoon of organisatie. Nummer en naam kloppen. Het bericht is nauwelijks van echt te onderscheiden. U wordt gevraagd direct iets te betalen of te doen.
  Bij twijfel: reageer niet en klik niet op een link. **Bel** zelf met de u bekende organisatie om te verifiëren.

VRIEND OF FAMILIELID IN NOOD

Dringend geld nodig!

- **Bekende truc**
  Een kind, vriend of familielid stuurt een bericht dat er **dringend financiële** hulp nodig is. Vaak in het buitenland en met allerlei problemen, zoals pinpas kwijt of telefoon defect. De ‘bekende’ vraagt u om snel geld over te maken. Trap er niet in!
- Soms blijkt het account van de het familielid of de bekende gehackt te zijn. Of gebruikt de oplichter een vals account of een nieuw telefoonnummer.
- Neem altijd contact op met de degene die het bericht stuurde als er een dergelijk verzoek binnenkomt. Vaak via WhatsApp of SMS.

PREVENTIEMAATREGELEN

Belangrijke tips

- **Updates software**

  Updates van uw software zijn belangrijk om te zorgen dat het veilig blijft. Stel uw computer, smartphone of tablet zodanig in dat de updates altijd geïnstalleerd worden.

- **Free Wifi**

  Let op bij ‘gratis’ internet, op een terras, restaurant of dergelijke. Dit is NIET veilig. Deze ‘open’ wifi internet beschermd u niet voor personen die uw telefoon willen hacken. Ze kunnen ‘meekijken’.

- **Virusscanner**

  Gebruik een goede virusscanner. Deze worden vaak door uw internetaanbieder aangeboden.

MALWARE EN BLOKKEREN

Voorkom beschadiging van uw computer

- **Malware**
  Dat is software die specifiek is ontwikkeld om een computer binnen te dringen. Het kan gevoelige informatie van uw computer stelen, uw computer vertragen of beschadigen en zelfs nepmails versturen vanuit uw e-mailaccount zonder uw medeweten. Gebruik hiertegen de eerder genoemde VIRUSSCANNER.

- **Blokkeren ongewenste mails en spam**
  Voor blokkeren van ongewenste mails op *Gmail:* klik hier
  Voor het blokkeren van ongewenste mails op *Outlook:* klik hier

WACHTWOORDEN

Zwakke en sterke wachtwoorden

- **Sterke wachtwoorden**
  Het is belangrijk dat u ‘sterke’ wachtwoorden gebruikt. Er zijn meerdere mogelijkheden om hier goed mee om te gaan.

- Gebruik tweetrapsverificatie. Vaak via een code naar uw telefoon. Klik hier om er meer over te lezen.

- Test hier hoe lang het duurt uw wachtwoord te kraken.

- **TIP:** Maak door middel van een eenvoudige zin een wachtwoord. Liefst met een vreemd teken en een cijfer. Een spatie er tussen is prima. Bijvoorbeeld:
  - Ik heb een G@zelle herenfiets
  - Mijn 1e auto was een R&nault

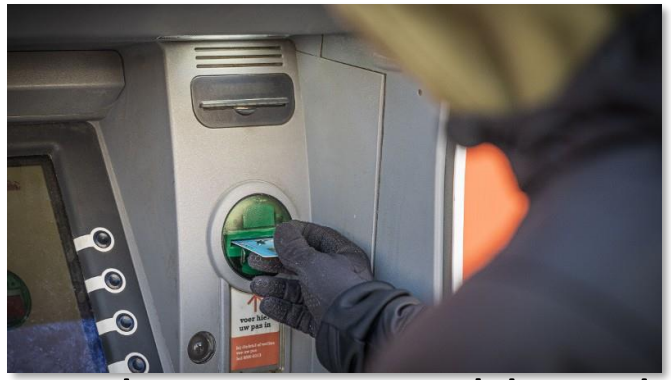
WACHTWOORDEN

Onthouden en veilig opslaan

- 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
- Google 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

CASH OF CARD TRAPPING GELDAUTOMAAT

Let op, blijf bij de geldautomaat



- **Cash trapping**
  Bij cash trapping manipuleren dieven de geldautomaat zodat er geen geld uit de machine komt. Zodra u dan 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?**
  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 dus bij de automaat staan, terwijl u belt. Dan kunnen de criminelen niet bij uw geld.

BELANGRIJKE en VEILIGE WEBSITES

https://www.blue-professionals.nl/voorlichtingsbijeenkomsten-senioren/

https://www.fraudehelpdesk.nl/https://veiliginternetten.nl/

https://www.seniorweb.nl/

https://www.veiligbankieren.nl/

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

https://www.maakhetzeniettemakkelijk.nl/

WANNEER BELT U 0900-8844 OF 112 ?

112

Alleen 112 bij **spoedeisende** zaken!

Bijvoorbeeld:

- bij levensbedreigende situaties
- als u een misdrijf ziet
- bij verdachte situaties
- u heeft tóch met die ‘bankmedewerker’ een afspraak gemaakt.

0900-8844

Bel 0900-8844 bij overige zaken**.**