ALV 2024 BPV ‘de Ploeg’

INFORMATIE OVER DIGITALE WEERBAARHEID EN VEILIGHEID

Wijkagenten Laren: Remco Wessels en Michelle Kamerbeek

2024

DEEL 1

BABBELTRUCS - OPLICHTERS AAN DE DEUR

Deze presentatie is gebaseerd op het naslagwerk van Maarten Keijzer van Blue Professionals www.blue-professionals.nl

1. **Pakketbezorgers**: Kijk goed aan wie het pakket is gestuurd. Betaal (pinnen) nooit iets aan de deur. Maak met uw buren afspraken over het aannemen van een pakket.
2. **Aanbellen:** Men kan vragen te mogen telefoneren, de wc te gebruiken of water te drinken. Dit kan AFLEIDING zijn om een tweede persoon binnen te laten voor diefstallen. Aanbellen in de avonduren: NIET direct de deur openen. Gebruik een kierstandhouder, een deurspion of deurbelcamera. KIJK eventueel vanaf de eerste verdieping wie aan de deur staat.

Kierstandhouder: Let op dit keurmerk SKG v

Deurbel en spion, kijk op internet.

Deze heeft GEEN Keurmerk ➔

BANKPAS EN PINNEN

Als u geld wilt pinnen, doe dit dan liefst in een winkel in plaats van op straat

Pinnen in de winkel of bij de automaat

- Scherm uw pincode af en laat geen mensen meekijken.
- Laat u niet afleiden.
- Als er iemand te dicht bij u staat vraag dan afstand te houden.
- Berg uw bankpas en geld goed op. Vertrek pas als u klaar bent, ook al is het druk.

PHISHING, CYBERCRIME

Hengelen naar persoonlijke gegevens

- **Phishing** is ‘hengelen’ naar persoonlijke gegevens. Criminelen sturen u een e-mail om te proberen inloggegevens, creditcardinformatie, pincodes, bankrekeningnummers of naw- gegevens te achterhalen.
- Phishingmails lijken bedrieglijk echt. Bij twijfel ➔bel naar de afzender.
- Soms staat er een ‘fout’ in een webadres en wordt u gevraagd dit foute adres te gebruiken. U komt dan uit bij criminelen.
- www.anbw.nl i.p.v. www.anwb.nl
- www.rab0.nl i.p.v. www.rabo.nl

PHISHING

Hengelen naar persoonlijke gegevens

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

- Klik **nooit** op een link of bijlage in de e-mail als u het niet vertrouwt. Als u dit wel doet, kan er ongemerkt een kwaadaardig programma op uw computer worden geïnstalleerd.

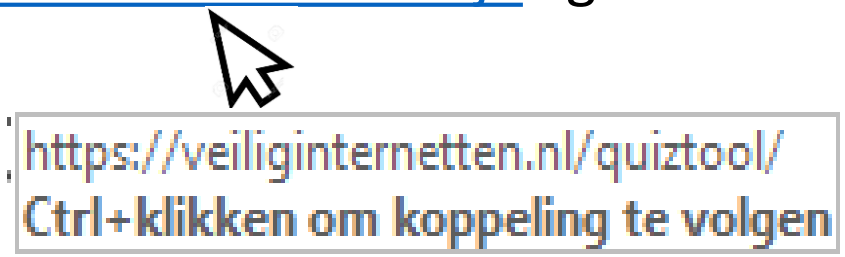
PHISHING (3)

Hengelen naar persoonlijke gegevens

- U kunt via een quiz controleren of u kennis heeft van phishing.
  Voor deze quiz en meer quizzen:

  https://veiliginternetten.nl/quiztool/

- Tekst van een link kan worden veranderd: wat hier achter zit kan alles zijn ga met de cursor op de link staan en u ziet wat er achter zit



Melden van phishing:

- Als u een phishing mail heeft ontvangen, dan kunt u dit melden bij de fraudehelpdesk: https://www.fraudehelpdesk.nl/ U kunt de mail ook doorsturen naar uw bank.

HET SLOTJE NAAST DE ADRESBALK

Beveiligde websites

- Tegenwoordig zijn de meeste websites beveiligd.

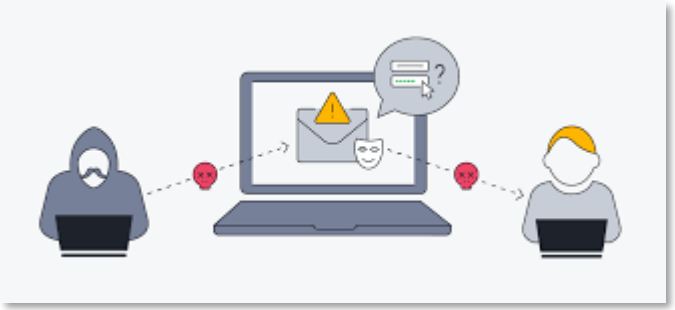
- Er staat dan in de *adresbalk* een **s** (http**s**), of een zwart slotje.
  Voorbeeld van beveiligde webadres: https://www.politie.nl/

- https staat voor SLL (Secure Socket Layer) en voorkomt dat gegevens tussen u en de webserver worden gestolen.

- Klik hier voor meer info over het slotje.

https://verbeterjewebsite.nl/wat-betekent-het-slotje-naast-de-adresbalk/
Ctrl+klikken om koppeling te volgen

BANKHELPDESKFRAUDE



Bij deze oplichtingstruc bellen fraudeurs mensen thuis op en doen zich voor als bankmedewerkers. U krijgt te horen dat uw bankrekening is gehackt en er geld naar het buitenland is overgemaakt. Gelukkig heeft de bank de transactie onderschept. Hierna gaat de medewerker u helpen om erger te voorkomen. Ze vragen bijvoorbeeld inlogcodes of dat u uw bankpas met pincode afgeeft…….en zo helpen ze u van uw geld af.

Het patroon is: BANG maken en hierna HELPEN

BANKHELPDESKFRAUDE

Herkennen

- Een bank zal u 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 nóóit onder druk zetten. Een bank heeft namelijk zelf de mogelijkheid om een rekening te blokkeren als dat nodig is.

BANKHELPDESKFRAUDE

Wat moet ik doen?

- Verbreek direct de verbinding. Bel niet terug.

- Bel dan zelf uw bank via een algemeen bekend nummer. 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.

BANKHELPDESKFRAUDE

Wat moet ik doen als ik al slachtoffer ben?

- Aangifte doen bij de politie.
  Een afspraak maken kan via nummer **0900-8844**.
- Heeft u een afspraak gemaakt uw bankpas op te laten halen bel dan direct **112.**
- Neem ook direct contact op met uw bank.

TELEFOONNUMER SPOOFING

Ander telefoonnummer aannemen door crimineel

- Bij **spoofing** met telefoonnummers neemt de oplichter een *ander telefoonnummer* aan. U ziet dan in uw scherm een telefoonnummer dat bij uw bank hoort. Maar het is NEP. Dit wordt veel gebruikt bij helpdeskfraude, waarbij oplichters u bellen namens een helpdesk van banken, andere grote bedrijven en zeer bekend Microsoft.
- Ze proberen u bijvoorbeeld ertoe aan te sporen de controle over uw computer te geven, zogenaamd om een bepaalde ‘bug’ te verhelpen.
- **Oplichting - bankfraude**. Klik hier om het filmpje te bekijken.

EMAIL SPOOFING

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

- Let altijd op een correct e-mailadres van de afzender: @bedrijfsnaam.nl
  - Dit is goed: janjansen@abnamro.nl -
  Dit is fout: janjansen@abnamr0.nl
- Handige fraudeurs maken gebruik van **'e-mail spoofing'**. 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 waar de link naartoe leidt door met de cursor op de link te gaan staan zonder te klikken.

>>>> DEEL 2 wordt opgenomen in de volgende Nieuwsbrief.