it Skeakeltsje

Secretariaat: Mevrouw Tilly Smidt
Zijlroede 59, 8446 MS HEERENVEEN
0513-785122 info@kbo-fryslan.nl
Website: www.KBO-Fryslan.nl
IBAN NL90INGB0006583245 tnv KBO Fryslan
Ledenadministratie: leden@kbo-fryslan.nl
Kopij of informatie: info@kbo-fryslan.nl
Wij versturen zelf mail vanaf: friesland@leaweb.nl en info@kbo-fryslan.nl

Senioren
KBO Fryslân

Cybercriminaliteit

Cybercriminaliteit/ Lekken van data.
Zoals u regelmatig hoort en kunt lezen worden er gegevens buit gemaakt door internet- oftewel door cybercriminelen. Hierdoor kunnen vreemden uw naam, adres, telefoonnummer en soms zelfs bankgegevens of uw paspoortnummer hebben.
Deze criminelen gebruiken deze gegevens vervolgens om u te benaderen, vaak per mail of telefoon en u ervan te overtuigen dat ze van een bank, of bedrijf zijn.

Tip: Bent u klant van het bedrijf (geweest), dan kunt u op politie.nl/informatie/checkjehack.html controleren of uw gegevens ook in de gestolen data zitten.

Ouderen zijn vaker doelwit van cybercrime, wat grote emotionele en financiële gevolgen kan hebben. Het is van groot belang waakzaam te zijn en waar mogelijk, uw digitale vaardigheden te verbeteren. Hier zijn de belangrijkste adviezen om veilig te blijven:

- Herken de trucs van criminelen (phishing en spoofing)
- Wees kritisch: Vertrouw geen e-mails, WhatsApp-berichten of telefoontjes waarin wordt gevraagd om direct geld over te maken of persoonlijke gegevens te delen.
- Banken, politie of overheidsinstanties (zoals de Belastingdienst) vragen **nooit** via telefoon of e-mail om inlogcodes, pincodes of het overboeken van geld naar een 'veilige rekening'. Ze zullen ook nooit zeggen dat ze iemand langs zullen sturen om uw waardevolle bezittingen veilig te stellen!
- Spoofing: Oplichters kunnen het telefoonnummer van een bank vervalsen, waardoor het lijkt alsof de bank echt belt. Hang bij twijfel op en bel zelf terug via het officiële nummer. Belangrijke zaken zal de bank u per brief mededelen.
- Wachtwoorden: Gebruik voor elke site een ander, sterk wachtwoord. Gebruik bij voorkeur een wachtwoordmanager.
- Tweestapsverificatie: Schakel extra beveiliging (tweestapsverificatie) in, waarbij je naast een wachtwoord ook een code via SMS of app nodig hebt.

- Houd computer, tablet en smartphone up-to-date. Updates dichten beveiligingsgaten.
- Krijgt u een WhatsApp-bericht van een 'bekende' die een nieuw nummer heeft en dringend geld nodig heeft? Dit is een bekende oplichterstruc. Bel die persoon eerst op via het oude nummer om te verifiëren of het klopt.
- Krijgt u een mailtje waarin u onder druk gezet worden een factuur te betalen? Kijkt u eerst rustig na of dit wel klopt. Er gaan al diverse mailtjes rond zogenaamd van Infomedics of van het CJIB maar die kloppen niet altijd.

Cybercriminaliteit

- Belangrijk.
  Laat nooit onbekenden binnen, hoe betrouwbaar ze ook lijken en hoe mooi hun verhaal ook is.
  Vraag altijd om legitimatie, ook bij mensen die beweren van de bank of een nutsbedrijf te zijn. Ook dit is een bekende oplichterstruc. De bank stuurt nooit zomaar een medewerker naar u toe en ook uw eigen energiemaatschappij niet. En de politie zal nooit voor de bank of een ander bedrijf iets voor u ophalen om te bewaren!
- Criminelen worden steeds slimmer en zijn erg goed in mensen subtiel onder druk te zetten. U hoeft u niet te schamen als u slachtoffer bent. U treft geen blaam.
- Meld het direct: Doe altijd aangifte bij de politie (0900-8844) en meld fraude bij de Fraudehelpdesk (088-786737Bank inlichten: Heeft u geld overgemaakt? Neem direct contact op met uw bank.
- Het meest veilige is om zogenaamde bedrijven niet telefonisch te woord te staan en bij twijfel kunt u zeggen dat u zelf even met het bedrijf gaat bellen (naar het nummer dat bij u bekend en vertrouwd is).
- Geef nóóit wachtwoorden of pincodes door! Geef nooit uw bezittingen af.
- Facturen: criminelen kunnen misbruik maken van de situatie door valse facturen te sturen die lijken te komen van uw telecomprovider , CJIB, tandarts of andere bedrijven. Controleer de afzender en vergelijk bedragen met eerdere facturen. **Facturen van uw telecomaanbieder kunt u altijd inzien in uw persoonlijke account op de officiële website. Bij twijfel, neem zelf contact op met de organisatie. Met dit soort nep facturen jagen ze mensen een vorm van angst aan (incassokosten) waardoor men gauw geneigd is te betalen. Niet doen: altijd eerst checken!**
- Door kritisch te blijven en verdachte situaties direct te checken, verkleint u de kans dat criminelen misbruik maken van u maken.