Veilig online

de Bibliotheek West-Brabant

→ Algemene tips tegen online fraude:

Bankpasfraude/helpdeskfraude:
De bank belt je omdat er verdachte transacties zijn op je rekening:

- De bank belt nooit om te vragen om een bankpas of pincode.
- Kluisrekeningen bestaan niet.
- Installeer nooit programma's waardoor anderen mee kunnen kijken!
- Bij twijfel: bel altijd politie.
- Zoek zelf het nummer van de bank op en bel terug.

Phishing via SMS of e-mail:
Je ontvang een sms of e-mail van een bedrijf /organisatie waarbij je moet klikken op een link voor een betaling of om het bericht te lezen. Een betaalverzoek van onbekenden via WhatsApp valt hier ook onder. (Vaak berichten met paniek en er is snel actie nodig)

- Klik nooit op linkjes in e-mails of berichten.
- Wat kan je wèl doen? Ga naar de officiële website of app en log daar in.
- Zoek het telefoonnummer op via internet (niet het nummer uit het bericht gebruiken!) en bel de bank/bedrijf.
- Check de afzender: klopt het e-mailadres?
- Check de link van de website: is deze wel echt van het bedrijf/organisatie?
- Whatsapp betaalverzoek: Bel de persoon eerst voordat je geld overmaakt.

Veilige wifi:
Als je verbinding maakt met het openbare wifi-netwerk van een hacker, kan hij bij jouw bankzaken.

- Check goed met welke wifi je automatisch bent verbonden.
- Een wachtwoord maakt wifi niet automatisch veilig.
- De naam van het netwerk zegt niets over de eigenaar van het netwerk.
- Als je wel op een openbare wifi zit: doe geen bankzaken en log nergens in.
- Doe bankzaken altijd via de app, die is veiliger dan de website.

'Voice cloning' (= stem namaken voor fraude) of WhatsApp fraude:
Een familielid belt je op in paniek, dat er iets is gebeurd en dat ze snel geld nodig hebben.

- Vraagt de persoon om geld? = een rode vlag!
- Is er spoed bij? = een rode vlag!
- Bel altijd zelf terug naar die persoon, via het nummer dat je al had. (Of videobellen!)
- Spreek een codewoord af met je familie, als je geld moet overmaken.
- Bel de politie!

Veilige wachtwoorden:

- Gebruik voor elke account een ander wachtwoord.
- Gebruik minimaal 15 karakters.
- Gebruik een wachtwoordzin, makkelijk om te onthouden.
- Gebruik letters, symbolen, cijfers en hoofdletters.
- Je kan een online wachtwoordmanager aanzetten/installeren.
- Of noteer alle wachtwoorden in een adresboekje (berg het wel goed op!)

Bitcoin Fraude:

- Vertrouw geen onverwacht aanbod.
- Een 'nu of nooit' actie is nooit betrouwbaar.
- Check of je bitcoin in eigen beheer blijft.
- Nooit je privé sleutel geven.
- Check of het bedrijf betrouwbaar is.

Algemene tips:

- Zorg dat je updates gelijk installeert.
- Zorg voor up-to-date antivirus software.
- Maak unieke + lange wachtwoorden.
- Zorg voor offline bestanden als back-up (op een externe harde schijf).
- Maak een noodplan, zodat je weet wat je moet doen als je gehackt bent.

→ Handige websites:

Wil je meer leren over je computer/telefoon:
https://www.bibliotheekwb.nl/activiteiten/aanmeldformulieren/ik-wil-leren.html

Omschrijving/ organisatie	Link
Je beschermen tegen online fraude	https://zowerktfraude.nl/ https://laatjeniethackmaken.nl/
Check of je e-mailadres al gevonden is in een hack	https://www.politie.nl/informatie/checkjehack.html
Online veiligheid	https://www.maakhetzeniettemakkelijk.nl
Hackhelpdesk	https://www.hackhelpdesk.nl/
Tips voor veilig internetten	https://veiliginternetten.nl/
Veilig wachtwoorden en wifi:	https://www.bibliotheekwb.nl/leren/digiwegwijs.html
Quiz: kan je phishing herkennen?	https://veiliginternetten.nl/quiztool/alert-online-echt-nep-quiz/

Heb je nog vragen, mail ze naar: digiwegwijs@bibliotheekwb.nl of
m.liefting@bibliotheekwb.nl