Marieke Liefting
Consulent digitale geletterdheid
m.liefting@bibliotheekwb.nl

de Bibliotheek West-Brabant

Veilig online

➔ Algemene tips tegen online fraude:

Bankpasfraude/helpdeskfraude:
Wordt je gebeld door bank 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 vreemden mee kunnen kijken!
- Bij twijfel: bel altijd politie.
- Zoek zelf het nummer van de bank op en bel terug.
- Verlaag het daglimiet van je rekening.

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 van vreemden.
- Wat kan je wél 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 wel?
- Check de link van de website: is deze wel echt van het bedrijf/organisatie?
- Wordt jij als klant ook bij naam genoemd? Phishing is namelijk altijd anoniem.
- Whatsapp betaalverzoek: Bel de persoon eerst voordat je geld overmaakt.
- Heb je jezelf ooit aangemeld bij het bedrijf, dan kan je jezelf ook uitschrijven. Bij phishing werkt dit niet. Verwijder de mail of verplaats hem naar de folder met spam.

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

- Check goed met welk wifi-netwerk 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.

z.o.z.

Veilige wachtwoorden:

- Gebruik voor elke account een ander wachtwoord.
- Gebruik minimaal 12 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!)

Algemene tips:

- Zorg dat je updates voor computer en telefoon gelijk installeert.
- Zorg voor up-to-date antivirus software op je computer.
- Antivirus software voor je telefoon is niet nodig.
- 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.

Nep agenten aan de deur:

- Let op; Soms worden ze telefonisch aangekondigd.
- Vraag de agenten om een politielegitimatiebewijs.
- = dit is een fysieke pas, het formaat van een creditcard.
- Ook in burgerkleding heeft een agent dit bewijs altijd bij zich.
- Bel de politie en check het nummer van de legitimatie.
- Laat niemand binnen totdat je zeker weet dat het klopt.

➔ Handige websites:

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
Tips voor veilig internetten	https://veiliginternetten.nl/
Veilige wachtwoorden en wifi:	https://www.bibliotheekwb.nl/leren/digiwegwijs.html
Quiz: kan je phishing herkennen?	https://veiliginternetten.nl/quiztool/alert-online-echt-nep-quiz/

We organiseren allerlei leuke workshops, lezingen en activiteiten voor digitale geletterdheid in de bibliotheek.
Neem een kijkje in de agenda, die staat op onze website www.bibliotheekwb.nl

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