

SAMENVATTING HOOFDSTUK 1

Digiveilig en Mediawijs

Aan het eind van alle lesbrieven ben je **digiveilig en mediawijs**: je weet dan hoe je veilig moet omgaan met je computer, je smartphone, je tablet en het internet.

Wachtwoorden

Een **wachtwoord** zorgt ervoor dat je informatie veilig kunt opbergen.

Je moet er veilig mee omgaan.

Je moet het niet zomaar aan iedereen geven.

Kies altijd een sterk wachtwoord.



Sterke wachtwoorden

Kenmerken van een sterk wachtwoord zijn:

- Het is niet makkelijk door anderen te raden;
- Je kunt het zelf wel makkelijk onthouden;
- Het heeft tenminste 8 tekens, het liefst 14;
- Het bestaat uit zowel hoofdletters, kleine letters, cijfers en leestekens;
- Je moet het regelmatig veranderen.

Een eenmalig wachtwoord



Een **eenmalig wachtwoord** krijg je bijvoorbeeld als je ergens een account aanmaakt.

Ook als je je wachtwoord bent vergeten en het weer opvraagt, krijg je er meestal een.

Het is een wachtwoord dat bestaat uit een aantal tekens dat je kunt gebruiken om weer in te loggen.

Daarna moet je je wachtwoord meteen weer veranderen in iets dat je zelf hebt gekozen.

Computercriminaliteit

Er zijn veel vormen van **computercriminaliteit**.

Meestal proberen computercriminelen een computer binnen te dringen en persoonlijke gegevens te achterhalen.

Dat achterhalen van gegevens doen ze bijvoorbeeld met een Trojan of Spyware.



Ook nemen ze computers 'over'. De computer wordt dan gebruikt voor:

- Bedreigingen via sociale netwerken;
- Fraude;
- Oplichting;
- Heling;
- Witwassen;
- Bedrijfsspionage.

Inbreken in de computer

Er zijn 2 soorten inbrekers:

1. **Hackers**

Hebben goede bedoelingen.

Hacken is voor hen een sport en het doel is om ontwikkelaars te wijzen op beveiligingslekken.

2. **Crackers**

Hebben kwade bedoelingen.

Willen bijvoorbeeld bankgegevens achterhalen. Ze doen het alleen om er zelf beter van te worden.

Gegevens achterhalen

Criminelen bellen je op om achter je gegevens te komen.

Ze gebruiken een babbeltruc.

Ze doen zich dan bijvoorbeeld voor als iemand van de bank. Ze proberen je inloggegevens voor online bankieren te weten te komen.



Dat is **Pretexting**.

Criminelen richten zich daarbij op mensen. Mensen zijn de zwakste schakel in de computerbeveiliging.

Malware

Ga nooit in op **advertenties** voor **gratis software** op internet. Hetzelfde geldt voor pop-ups met de melding dat je een **prijs gewonnen** hebt.

Als je daarop klikt wordt er vaak software gedownload waarmee **malware** of een **virus** meelift.



Malware kun je verdelen in:

1. **Spyware**

Spyware is 'spionagesoftware'. Het stuurt allerlei gegevens over je computergebruik door naar anderen.

2. **Adware**

Adware haalt reclame naar iemands computer. Daardoor verschijnen er extra banners en pop-ups.

Phishing



Via **Phishing** kunnen kwaadwillenden achter jouw gegevens komen.

Je krijgt bijvoorbeeld een **e-mail** van je 'bank'.

Daarin wordt gevraagd om in te loggen op de website.

Als je klikt op de link, kom je niet op de website van je bank, maar op een andere website.

Computercriminelen kunnen dan bijvoorbeeld:

- je informatie verkopen;
- je identiteit stelen;
- geld van je bankrekening halen;
- contacten aanvallen.