Inhoudsopgave Algemene module Digiveiligheid

Het gebruik van ICT in ons dagelijks leven is vanzelfsprekend geworden. Maar zijn we ons voldoende bewust van de mogelijke gevaren? Cybercriminaliteit is een sterk groeiend fenomeen en komt in vele vormen voor. Hackers, phishing, skimming, etc. Het is dagelijks in het nieuws.

In de module Digiveiligheid maakt u kennis met de meest voorkomende gevaren en leert u hiermee omgaan. Onderwerpen als veilig surfen en communiceren, zorgvuldig omgaan met persoonlijke gegevens en gebruik van een beveiligd netwerk komen hierin aan de orde.

Studiebelasting: 14-18 uur

Hieronder staan de onderwerpen die in deze module behandeld worden:

Veiligheid, omgang en kwaadaardige software

- Digiveiligheid
- Gegevens en informatie
- Cyberpesten
- Nettiquette
- Malware
- Firewall
- Computercriminaliteit
- Kopen via internet
- Webshopkeurmerk
- Virussen
- Anti-virusprogramma's
- Beveiligen van je smartphone
- Beveiliging tegen diefstal

Illegaal verkrijgen van gegevens

- Hacken en cracken
- Pretexting
- Phishing
- Information Diving
- Skimmen
- Pharming
- Beveiligde website
- Bedreigingen
- Keylogging
- Geldezel
- Shoulder surfing

Identiteit en wachtwoorden

- Identiteitsfraude
- Wettelijke sancties
- DigiD
- Identiteit vaststellen
- Digitale handtekening
- Veilig omgaan met je wachtwoord
- Sterke wachtwoorden
- Een eenmalig wachtwoord en wachtwoordmanager
- Een betrouwbaar bedrijf
- Vertrouwen

Contact, privacy en cookies

- Instant Messaging
- Veilig chatten
- Grooming
- Niets te verbergen
- Persoonlijke gegevens op internet
- Privacy-instellingen bij sociale media
- Spam op sociale media
- Automatisch aanvullen
- Cookies
- Cookies verwijderen
- Cookiewetgeving

Toezicht, netwerken en bestanden

- Filtersoftware
- Ouderlijk toezicht
- Netwerk
- De netwerkbeheerder
- Draadloos netwerk
- Beveiliging draadloos netwerk
- Beveiliging in- of uitschakelen
- Bestanden beveiligen
- Versleutelen
- Overmacht
- Een back-up
- Bestanden vernietigen