Digi-veiligheid

In deze module worden begrippen uiteengezet die betrekking hebben op een veilig gebruik van ICT in het dagelijks leven en komen de vaardigheden aan de orde die worden gebruikt om een beveiligde netwerkverbinding te onderhouden, het internet veilig te gebruiken, en gegevens en informatie op een passende manier te beheren.

Doel van de module

De kandidaat:

- Begrijpt het belang van beveiliging van informatie en gegevens, en kan algemene principes op het gebied van bescherming, behoud en beheer van gegevens/privacy benoemen.
- Herkent gevaren van identiteitsdiefstal voor de persoonlijke veiligheid, en potentiële gevaren van het gebruik van cloud computing voor gegevens.
- Kan wachtwoorden en encryptie/versleuteling gebruiken om bestanden en gegevens te beveiligen.
- Begrijpt het gevaar van malware en kan een computer, een mobiel device of een netwerk beveiligen en malware-aanvallen weerstaan.
- Herkent veelgebruikte typen beveiliging van (draadloze) netwerken en kan persoonlijke firewalls en hotspots gebruiken.
- Kan een computer of device beschermen tegen ongeoorloofde toegang en is in staat wachtwoorden op een veilige manier te beheren en bij te werken.
- Kan geschikte browserinstellingen gebruiken en begrijpt hoe verificatie van websites en veilig internetten in zijn werk gaat.
- Begrijpt de beveiligingsproblemen bij communicatie die een rol spelen bij het gebruik van e-mail, sociale netwerken, Voice-over-Internet-Protocol, Instant Messaging en mobiele devices.
- Kan back-ups van gegevens op lokale en cloudopslaglocaties maken en terugzetten, en kan gegevens en apparatuur veilig verwijderen.

Categorie	Kennisgebied	Ref.	Kennisonderwerp
1 | Beveiligings-begrippen	1.1 | Gegevensbe-dreigingen	1.1.1	Het verschil kennen tussen gegevens en informatie.
		1.1.2	Weten wat de termen ‘cybercrime’ en ‘hacking’ inhouden.
		1.1.3	Herkennen van kwaadaardige en onopzettelijke bedreiging van gegevens afkomstig van personen, serviceproviders, externe organisaties.

Categorie	Kennisgebied	Ref.	Kennisonderwerp
		1.1.4	Herkennen van bedreiging van gegevens door uitzonderlijke omstandigheden zoals: brand, overstroming, oorlog, aardbevingen.
		1.1.5	Herkennen van bedreiging van gegevens door gebruik van cloud computing zoals: beperkte toegang, potentieel verlies van privacy.
	1.2 | Waarde van Informatie	1.2.1	De basiskenmerken van gegevensbeveiliging kennen, zoals: vertrouwelijkheid, integriteit, beschikbaarheid.
		1.2.2	Begrijpen waarom persoonlijke informatie wordt beveiligd, bijv. voorkomen van identiteitsdiefstal en fraude, behoud van privacy.
		1.2.3	Begrijpen waarom werkinformatie op computers en apparaten moet worden beveiligd: voorkomen van diefstal, frauduleus gebruik, onopzettelijk gegevensverlies, sabotage.
		1.2.4	Herkennen van algemene principes voor bescherming, behoud en beheer van gegevens/ privacy zoals: transparantie, legitieme doeleinden, proportionaliteit.
		1.2.5	Begrijpen van de termen ‘betrokkene’ en ‘verantwoordelijke’ met betrekking tot gegevens en weten hoe principes voor bescherming, behoud en beheer van gegevens/privacy daarop van toepassing zijn.
		1.2.6	Het belang kennen van naleving van richtlijnen en beleidsregels voor ICT-gebruik en de manier waarop die geraadpleegd kunnen worden.
	1.3 | Persoonlijke beveiliging	1.3.1	Begrip van de term ‘social engineering’ en de implicaties daarvan zoals: ongeoorloofde toegang tot computers en devices, ongeoorloofd verzamelen van gegevens, fraude.
		1.3.2	Herkennen van methoden van ‘social engineering’, zoals: telefoontjes, phishing, ‘shoulder surfing’.
		1.3.3	Weten wat de term identiteitsdiefstal inhoudt en de gevolgen kennen, zoals: persoonlijke, financiële, zakelijke en juridische gevolgen.

Categorie	Kennisgebied	Ref.	Kennisonderwerp
		1.3.4	Herkennen van methoden van identiteitsdiefstal, zoals 'information diving' (zoeken naar informatie op afgedankte gegevensdragers), skimmen en pretexting
	1.4 | Bestandsbeveiliging	1.4.1	Begrijpen wat het effect is van het in- of uitschakelen van macrobeveiligingsinstellingen.
		1.4.2	Begrijpen wat de voordelen en beperkingen zijn van versleuteling. Weten wat het belang is van het niet openbaar maken van het wachtwoord, de sleutel, het certificaat voor versleuteling.
		1.4.3	Een bestand, map, schijfstation versleutelen.
		1.4.4	Bestanden zoals documenten, spreadsheets en gecomprimeerde bestanden beveiligen met een wachtwoord.
2 | Malware	2.1 | Typen en methoden	2.1.1	Weten wat de term 'malware' inhoudt. Herkennen van verschillende manieren waarop malware op computers en devices verborgen kan zijn, zoals: Trojaanse paarden, rootkits, achterdeuren.
		2.1.2	Besmettelijke malware herkennen en de werking ervan begrijpen, zoals: virussen en wormen.
		2.1.3	Soorten malware gericht op gegevensdiefstal en winstbejag/afpersing herkennen en begrijpen hoe ze werken, zoals: adware, ransomware, spyware, botnets, keylogging en diallers.
	2.2 | Bescherming	2.2.1	Begrijpen hoe antivirussoftware werkt en wat de beperkingen ervan zijn.
		2.2.2	Begrijpen dat antivirussoftware op computers en devices geïnstalleerd moet worden.
		2.2.3	Het belang inzien van geregeld updaten van de software zoals: antivirusprogramma's, plug-ins, toepassingen, besturingssysteem.
		2.2.4	Scannen van specifieke schijven, mappen en bestanden met antivirussoftware. Scans inplannen met behulp van antivirussoftware.
		2.2.5	Het risico begrijpen van het gebruik van verouderde en niet-ondersteunde software zoals: verhoogd risico op malware, incompatibiliteit.

Categorie	Kennisgebied	Ref.	Kennisonderwerp
	2.3 | Oplossen en verwijderen	2.3.1	Begrijpen wat de term ‘quarantaine’ inhoudt en wat het effect is van in quarantaine plaatsen van geïnfecteerde/verdachte bestanden.
		2.3.2	Geïnfecteerde/verdachte bestanden in quarantaine plaatsen, verwijderen.
		2.3.3	Begrijpen dat een malware-aanval kan worden opgespoord en tegengegaan met behulp van online informatiebronnen zoals: websites voor het besturingssysteem, antivirussoftware, browserfabrikanten en relevante instanties.
3 | Netwerk beveiliging	3.1 | Netwerken en verbindingen	3.1.1	De term ‘netwerk’ kennen en gangbare netwerken herkennen, zoals local area network (LAN), wireless local area network (WLAN), wide area network (WAN), virtual private network (VPN).
		3.1.2	Begrijpen wat het verbinden met een netwerk voor gevolgen heeft voor de beveiliging, zoals: malware, niet-geautoriseerde gegevenstoegang, behoud van privacy.
		3.1.3	Begrijpen wat de rol is van de netwerkbeheerder op het gebied van verificatie, autorisatie en accountbeheer, monitoren, installeren van relevante beveiligingspatches en updates, bewaken van het netwerkverkeer en aanpakken van malware binnen een netwerk.
		3.1.4	Begrijpen van de functie en beperkingen van een firewall in een persoonlijke en bedrijfsomgeving.
		3.1.5	Een persoonlijke firewall in- en uitschakelen. Een programma via een persoonlijke firewall toegang tot een service/voorziening geven of weigeren.

Categorie	Kennisgebied	Ref.	Kennisonderwerp
	3.2 | Draadloze beveiliging	3.2.1	Herkennen van verschillende opties voor draadloze beveiliging en hun beperkingen zoals: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA)/Wi-Fi Protected Access 2 (WPA2), filteren van Media Access Control (MAC), verbergen van Service Set Identifier (SSID).
		3.2.2	Begrijpen dat het gebruik van een onbeveiligd draadloos netwerk kan leiden tot aanvallen zoals: afluisteraars, netwerkkaping, man-in-the-middle-aanvallen.
		3.2.3	Weten wat de term 'persoonlijke hotspot' inhoudt.
		3.2.4	Een beveiligde persoonlijke hotspot in- en uitschakelen en devices veilig verbinding laten maken en verbreken.
4 | Toegangs beheer	4.1 | Methoden	4.1.1	Maatregelen bepalen voor het voorkomen van ongeoorloofde toegang tot gegevens zoals: gebruikersnaam, wachtwoord, pincode, versleuteling, meervoudige verificatie.
		4.1.2	Begrijpen van de term 'eenmalig wachtwoord' en het gebruik ervan.
		4.1.3	Begrijpen wat het doel is van een netwerkaccount.
		4.1.4	Begrijpen dat een netwerkaccount moet worden benaderd met een gebruikersnaam en wachtwoord en moet worden vergrendeld/afgemeld wanneer het niet in gebruik is.
		4.1.5	Herkennen van algemene biometrische beveiligingstechnieken die bij toegangsbeheer worden gebruikt, zoals: vingerafdrukken, irisscans, gezichtsherkenning, handgeometrie.
	4.2 | Wachtwoord-beheer	4.2.1	Herkennen van goed wachtwoordbeleid zoals: acceptabele wachtwoordlengte, acceptabele combinatie van letters, cijfers en speciale tekens, wachtwoorden niet delen en geregeld vernieuwen, verschillende wachtwoorden voor verschillende diensten.
		4.2.2	Begrijpen van de functie en beperkingen van software voor wachtwoordbeheer.

Categorie	Kennisgebied	Ref.	Kennisonderwerp
5 | Veilig internetgebruik	5.1 | Browser-instellingen	5.1.1	De juiste instellingen selecteren voor het in- of uitschakelen van automatisch aanvullen en opslaan bij het invullen van een formulier.
		5.1.2	Persoonlijke gegevens uit een browser verwijderen, zoals: browsegeschiedenis, downloadgeschiedenis, internetbestanden in de cache, wachtwoorden, cookies, gegevens voor automatisch aanvullen.
	5.2 | Veilig internetten	5.2.1	Begrijpen dat bepaalde online activiteiten (aankopen, bankieren) alleen ondernomen moeten worden op veilige webpagina's.
		5.2.2	Manieren kennen om de echtheid van een website te herkennen zoals: kwaliteit van het materiaal, actualiteit, geldige URL, informatie van bedrijf of eigenaar, contactgegevens, beveiligingscertificaat, validatie van domeineigenaar.
		5.2.3	Weten wat de term 'pharming' inhoudt.
		5.2.4	Begrijpen wat de functie is van de verschillende soorten inhoudscontrolesoftware zoals: software voor internetfilters, ouderlijk toezicht.
6 | Communicatie	6.1 | E-mail	6.1.1	Begrijpen wat het doel is van versleutelen, ontsleutelen van een e-mail.
		6.1.2	Weten wat de term 'digitale handtekening' inhoudt.
		6.1.3	Mogelijk frauduleuze e-mail en ongewenste e-mail herkennen.
		6.1.4	Algemene kenmerken van phishing herkennen: gebruik van namen van bonafide organisaties, mensen, valse webkoppelingen, logo's en merknamen, verzoeken om opgeven van persoonlijke gegevens.
		6.1.5	Weten dat pogingen tot phishing kunnen worden aangegeven bij de bestaande organisatie en relevante autoriteiten.
		6.1.6	Weten dat het gevaar bestaat een computer of device met malware te besmetten door het openen van een e mailbijlage met een macro of uitvoerbaar bestand.

Categorie	Kennisgebied	Ref.	Kennisonderwerp
	6.2 | Sociale netwerken	6.2.1	Begrijpen dat het belangrijk is geen vertrouwelijke gegevens of identificeerbare persoonlijke gegevens te openbaren via sociale netwerken.
		6.2.2	Weten dat passende accountinstellingen voor sociale netwerken moeten worden toegepast en geregeld moeten worden bijgewerkt zoals: privacy- en locatie-instellingen.
		6.2.3	Accountinstellingen voor sociale netwerken toepassen: privacy- en locatie-instellingen.
		6.2.4	De potentiële gevaren kennen van het gebruik van sociale netwerken, zoals: cyberpesten, grooming, kwaadwillige publicatie van persoonlijk materiaal, valse identiteiten, frauduleuze hyperlinks, materialen, berichten.
		6.2.5	Weten dat ongepast gebruik van sociale netwerken of gedrag kan worden gerapporteerd bij de serviceprovider en relevante autoriteiten.
	6.3 | VoIP en chatten	6.3.1	Begrijpen wat de veiligheidsrisico's zijn van chatberichten (Instant Messaging, IM) en van Voice over IP (VoIP) zoals: malware, toegang via de achterdeur, toegang tot bestanden, afluisteren.
		6.3.2	Herkennen van methoden om de vertrouwelijkheid tijdens het gebruik van chatten en VoIP te waarborgen, zoals: versleuteling, niet doorgeven van vertrouwelijke informatie, beperking van bestandsdeling.
	6.4 | Mobiel	6.4.1	De mogelijke implicaties begrijpen van het gebruik van apps van niet-officiële app-stores, zoals: mobiele malware, onnodige aanslag op resources, toegang tot persoonlijke gegevens, slechte kwaliteit, verborgen kosten.
		6.4.2	Weten wat de term 'toepassingsmachtiging' inhoudt.
		6.4.3	Weten dat mobiele apps persoonlijke informatie van het device kunnen halen zoals: contactgegevens, locatiegeschiedenis, afbeeldingen.
		6.4.4	Weten welke beveiligings- en voorzorgsmaatregelen er kunnen worden genomen in geval van verlies zoals: uitschakelen op afstand, wissen op afstand, device lokaliseren.

Categorie	Kennisgebied	Ref.	Kennisonderwerp
7 | Veilig gegevensbeheer	7.1 | Beveiligen en back-ups maken	7.1.1	Herkennen van manieren om de fysieke beveiliging van (mobiele) apparatuur te garanderen, zoals: niet onbewaakt achterlaten, registreren van de locatie en details van apparatuur, gebruik van kabelsloten, toegangsbeheer.
		7.1.2	Het belang inzien van een back-upprocedure bij verlies van gegevens van computers en devices.
		7.1.3	Herkennen van de kenmerken van een back-upprocedure zoals: regelmaat/frequentie, planning, opslaglocatie, gegevenscompressie.
		7.1.4	Back-ups maken naar een locatie zoals een lokale schijf, externe schijf/media, clouddienst.
		7.1.5	Back-ups terugzetten vanaf een locatie zoals een lokale schijf, externe schijf/media, clouddienst.
	7.2 | Veilig verwijderen en vernietigen	7.2.1	Het verschil kennen tussen verwijderen en permanent wissen van gegevens.
		7.2.2	Begrijpen wat de redenen zijn voor het permanent wissen van gegevens van schijven of apparaten.
		7.2.3	Weten dat verwijderen van content niet altijd permanent is op bijvoorbeeld sociale netwerken, internetfora en clouddiensten.
		7.2.4	Herkennen van algemene methoden voor het permanent wissen van gegevens, zoals: versnipperen, vernietigen van schijven/media, demagnetiseren, gebruik van hulpmiddelen voor gegevensvernietiging.