ECDL
NEDERLAND

SYLLABUS

SECURITY & PRIVACY
AWARENESS

Syllabus versie 2.O_NL

Doel

Dit document bevat de syllabus behorende bij de Security & Privacy Awareness test. In de syllabus worden aan de hand van leeruitkomsten de kennis en vaardigheden uiteengezet waarover een kandidaat voor de module Security & Privacy Awareness dient te beschikken. Ook staat de basis beschreven voor de theorie- en praktijktoets in deze module.

ECDL Nederland is onderdeel van de Nederlandse Associatie voor Examinering en internationaal verbonden aan de ECDL Foundation.

Vrijwaringsverklaring

Ofschoon ECDL Nederland deze publicatie met de grootste zorg heeft samengesteld, kan ECDL Nederland als uitgever geen garanties geven ten aanzien van de volledigheid van de hierin vervatte informatie, noch kan de ECDL Nederland verantwoordelijk worden gehouden voor eventuele fouten, omissies, onnauwkeurigheden, of eventueel verlies of schade die ontstaat door het gebruik van deze informatie of van instructies of advies uit deze publicatie.

ECDL Nederland behoudt zich het recht voor dit materiaal op elk moment zonder voorafgaande kennisgeving te wijzigen.

Contact: + 31 (0)33 75010 99, info@ecdl.nl

Module Security& Privacy Awareness

In deze module worden begrippen uiteengezet die betrekking hebben op een veilig gebruik van ICT in het dagelijks (werk)leven, de meest voorkomende aspecten van het begrip privacy en de wet datalekken. En komen vaardigheden aan de orde die worden gebruikt om 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 (persoons)gegevens.
- Kan algemene principes op het gebied van bescherming, behoud en beheer van gegevens/privacy benoemen.
- Herkent gevaren van identiteitsdiefstal voor de persoonlijke veiligheid.
- Kan wachtwoorden en encryptie/versleuteling gebruiken om bestanden en gegevens te beveiligen.
- Kan wachtwoorden op een veilige manier beheren en bijwerken
- Begrijpt het gevaar van malware en kan een computer, een mobiel device of een netwerk beveiligen tegen malware en malware-aanvallen weerstaan.
- Herkent veelgebruikte typen beveiliging van (draadloze) netwerken.
- Kan een computer of device beschermen tegen ongeoorloofde toegang.
- Kan uitleggen hoe verificatie van websites en veilig internetten werkt
- Begrijpt de beveiligingsproblemen bij communicatie die een rol spelen bij het gebruik van e-mail, sociale netwerken (Linked-In, facebook e.d.), Instant Messaging (Chatten, WhatsApp e.d.) en mobiele apparaten.
- Kan back-ups van gegevens op lokale opslag en cloud opslag maken en terugzetten.
- Kan gegevens en apparatuur veilig verwijderen.
- Kan aantonen op de hoogte te zijn van de van toepassing zijnde privacy wetgeving

CATEGORIE	KENNISGEBIED	REF.	KENNISONDERWERP
1 Beveiligingsbegrippen	*1.1 Gegevensbedreigingen*	1.1.1	Het verschil benoemen tussen gegevens en informatie.
		1.1.2	De betekenis van de termen ‘cybercrime’ en ‘hacking’ aangeven.
		1.1.3	Kwaadaardige en onopzettelijke bedreigingen van gegevens afkomstig van personen, serviceproviders, externe organisaties herkennen.
		1.1.4	Bedreiging van gegevens door uitzonderlijke omstandigheden zoals: brand, overstroming, oorlog, aardbevingen herkennen.

CATEGORIE	KENNISGEBIED	REF.	KENNISONDERWERP
		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 basale karakteristieken van informatiebeveiliging, zoals vertrouwelijkheid, integriteit en beschikbaarheid beschrijven.
		1.2.2	Uitleggen waarom persoonlijke informatie beveiligd moet worden, bijv. het voorkomen van identiteitsdiefstal en fraude, en het handhaven van privacy.
		1.2.3	Uitleggen waarom gegevens op computers en apparaten moet worden beveiligd bijvoorbeeld: voorkomen van diefstal, frauduleus gebruik, onopzettelijk gegevensverlies, sabotage.
		1.2.4	De algemene principes voor bescherming, behoud, beheer subsidiariteit gegevens/privacy benoemen.
	1.3 Persoonlijke beveiliging	1.3.1	Het begrip ‘social engineering’ en de implicaties daarvan begrijpen. Bijvoorbeeld zoals ongeoorloofde toegang tot computers en andere apparaten, ongeoorloofd verzamelen van gegevens, fraude
		1.3.2	Methoden van ‘social engineering’ herkennen zoals: telefoontjes, ‘phishing’, en ‘shoulder surfing’.
		1.3.3	Het begrip identiteitsdiefstal en de gevolgen daarvan begrijpen. Bijvoorbeeld persoonlijke, financiële, zakelijke en juridische gevolgen.
		1.3.4	Methoden van identiteitsdiefstal herkennen. Bijvoorbeeld: ‘information diving’ (zoeken naar informatie op afgedankte gegevensdragers), skimming en pretexting.
	1.4 Bestandsbeveiliging	1.4.1	Het gevolg van het in- of uitschakelen van macrobeveiligingsinstellingen beschrijven.
		1.4.2	De voordelen en beperkingen van versleuteling uitleggen.
		1.4.3	Een bestand, map, schijfstation, etc. versleutelen.

CATEGORIE	KENNISGEBIED	REF.	KENNISONDERWERP
		1.4.4	Bestanden zoals documenten, spreadsheets en gecomprimeerde bestanden met een wachtwoord beveiligen.
		1.4.5	Kan het belang van het niet openbaar maken van het wachtwoord, de sleutel of het certificaat voor versleuteling beschrijven.
2 Virus en malware	*2.1 Typen en methoden*	2.1.1	Beschrijven van de term ‘malware’.
		2.1.2	De werking van verschillende soorten malware uitleggen.
		2.1.3	Verschillende soorten malware: adware, ransomware, spyware, botnets, keylogging en diallers benoemen.
		2.1.4	Beschrijven van de term virus.
	2.2 Bescherming	2.2.1	Uitleggen hoe antivirussoftware en antimalware werkt.
		2.2.2	Uitleggen waarom antivirussoftware en antimalware op computers en devices geïnstalleerd moet worden.
		2.2.3	Uitleggen waarom regelmatig updaten van software belangrijk is. antivirusprogramma’s, antimalwareprogramma’s, plug-ins, toepassingen, besturingssysteem.
		2.2.4	Benoemen waarom periodiek scans moeten worden uitgevoerd.
		2.2.5	Uitleggen wat het risico is van het gebruik van verouderde en niet-ondersteunde software zoals: verhoogd risico op malware, incompatibiliteit.
		2.2.6	Beschrijven wat ‘quarantaine’ betekent en wat het effect is van in quarantaine plaatsen van geïnfecteerde/verdachte bestanden.
		2.2.7	Beperkingen van antivirussoftware en antimalware benoemen.

CATEGORIE	KENNISGEBIED	REF.	KENNISONDERWERP
3 Netwerkbeveiliging	*3.1 Netwerken en verbindingen*	3.1.2	De gevolgen voor de beveiliging bij het verbinden met een netwerk uitleggen. Bijvoorbeeld malware, niet-geautoriseerde gegevenstoegang, behoud van privacy.
		3.1.4	De functie en beperkingen van een firewall in een persoonlijke en bedrijfsomgeving beschrijven.
	3.2 Draadloze beveiliging	3.2.1	Herkennen van de verschillende opties en beperkingen van draadloze beveiliging en hun beperkingen herkennen 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	Ultleggen dat het gebruik van een onbeveiligd draadloos netwerk kan leiden tot aanvallen zoals: afluisteraars, netwerkkaping
		3.2.3	De betekenis van de term ‘persoonlijke hotspot’ uitleggen.
		3.2.4	Uitleggen hoe een beveiligde persoonlijke hotspot kan worden in- en uitgeschakeld om apparaten veilig verbinding te laten maken en te verbreken
4 Toegangsbeheer	*4.1 Methoden*	4.1.1	De maatregelen voor het voorkomen van ongeoorloofde toegang tot gegevens bepalen zoals: gebruikersnaam, wachtwoord, pincode, versleuteling, meervoudige verificatie.
		4.1.2	Beschrijven waarom en hoe een eenmalig wachtwoord wordt gebruikt.
		4.1.4	Uitleggen waarom een netwerkaccount moet worden benaderd met een gebruikersnaam en wachtwoord en moet worden vergrendeld/afgemeld wanneer het niet in gebruik is.
	4.2 Wachtwoorden	4.2.1	Een goed wachtwoordbeleid herkennen zoals: acceptabele wachtwoordlengte, acceptabele combinatie van letters, cijfers en speciale tekens, wachtwoorden niet delen en geregeld vernieuwen, verschillende wachtwoorden voor verschillende diensten.

CATEGORIE	KENNISGEBIED	REF.	KENNISONDERWERP
5 Veilig internetgebruik	*5.1 Browserinstellingen*	5.1.1	De juiste instellingen selecteren bij het invullen van een formulier voor het in- of uitschakelen van automatisch aanvullen en opslaan van (persoons)gegevens.
		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	Uitleggen waarom bepaalde online activiteiten (aankopen, bankieren) alleen ondernomen moeten worden op veilige webpagina's en veilige netwerken.
		5.2.2	Benoemen hoe de echtheid van een website herkend kan worden: inhoudelijke kwaliteit van het materiaal, actualiteit, geldige URL, informatie van bedrijf of eigenaar, contactgegevens, beveiligingscertificaat, validatie van domeineigenaar.
		5.2.4	Beschrijven van de functie van inhoudscontrolesoftware zoals: een internetfilter en ouderlijk toezicht.
	5.3 Browsen	5.3.1	Benoemen van de verschillen tussen cookies en kwaadaardige cookies.
		5.3.2	Beschrijven van de gevolgen van het gebruik van cookies.
		5.3.3	Inschatten van de gevolgen van het invullen van persoonsgegevens.
6 Communicatie	*6.1 E-mail*	6.1.1	Het doel van versleutelen en ontsleutelen van een e-mail uitleggen.
		6.1.2	De betekenis van 'digitale handtekening' benoemen.
		6.1.3	Eventuele frauduleuze e-mail, ongewenste e-mail herkennen.
		6.1.4	Kenmerken van phishing benoemen. Zoals: gebruik van namen van bonafide organisaties, mensen, valse webkoppelingen, logo's en merknamen, verzoeken om opgeven van persoonlijke gegevens.

CATEGORIE	KENNISGEBIED	REF.	KENNISONDERWERP
		6.1.6	De gevaren van het openen van een email-bijlage met een macro of uitvoerbaar bestand benoemen.
	6.2 Sociale netwerken	6.2.1	Uitleggen waarom het belangrijk is geen vertrouwelijke gegevens of identificeerbare persoonlijke gegevens te openbaren via sociale netwerken.
		6.2.3	De accountinstellingen voor sociale netwerken toepassen: privacy- en locatie-instellingen.
		6.2.4	De gevaren van het gebruik van sociale netwerken benoemen zoals: cyberpesten, grooming, kwaadwillige publicatie van persoonlijk materiaal, valse identiteiten, frauduleuze hyperlinks, materialen, berichten.
		6.2.5	Benoemen waar ongepast gebruik van sociale netwerken of gedrag kan worden gerapporteerd.
	6.4 Mobiele apparaten	6.4.1	De gevolgen van het gebruik van apps van niet-officiële app-stores beschrijven.
		6.4.3	Benoemen dat apps persoonlijke informatie van het apparaat kunnen halen zoals: contactgegevens, locatiegeschiedenis, afbeeldingen.
		6.4.4	Beveiligings- en voorzorgsmaatregelen die genomen kunnen worden in geval van verlies benoemen zoals: uitschakelen op afstand, wissen op afstand, device lokaliseren.
7 Veilig gegevensbeheer	*7.1 Beveiligen en back-ups maken*	7.1.1	Manieren om de fysieke beveiliging van (mobiele) apparatuur te garanderen benoemen, zoals: niet onbewaakt achterlaten, registreren van de locatie en details van apparatuur, gebruik van kabelsloten, toegangsbeheer.
		7.1.2	Het belang van een back-upprocedure benoemen.
		7.1.3	De kenmerken van een back-upprocedure benoemen zoals: regelmaat/frequentie, planning, opslaglocatie.

CATEGORIE	KENNISGEBIED	REF.	KENNISONDERWERP
		7.1.4	Back-ups naar een locatie zoals een lokale schijf, externe schijf/media, clouddienst maken.
		7.1.5	Terugzetten van back-ups vanaf een locatie zoals een lokale schijf, externe schijf/media, clouddienst.
	7.2 Veilig verwijderen en vernietigen	7.2.1	Het verschil tussen verwijderen en permanent wissen van gegevens benoemen.
		7.2.2	Het belang van het permanent wissen van gegevens van schijven of apparaten uitleggen.
		7.2.3	Uitleggen dat het verwijderen van materialen niet altijd definitief is op bijvoorbeeld sociale netwerken, internetfora en clouddiensten.
		7.2.4	Methoden voor het definitief vernietigen van gegevens benoemen zoals: versnipperen, vernietigen van schijven/media, demagnetiseren, gebruik van hulpmiddelen voor gegevensvernietiging.
8 Privacy	*8.1 Persoonsgegevens*	8.1.1	Het verschil tussen generieke en bijzondere persoonsgegevens benoemen.
		8.1.2	Het begrip privacy beschrijven.
	8.2 Informatiesysteem	8.2.1	Een informatiesysteem beschrijven.
		8.2.2	Het doel van een informatiesysteem benoemen.
		8.2.3	De term doelbinding beschrijven.
9 Organisatie	*9.1 Bedrijf*	9.1.1	De technische en organisatorische maatregelen die een bedrijf moet nemen op het gebied van privacy benoemen.
		9.1.2	Het doel van risico-analyse (Privacy Impact Assessment, PIA) benoemen.
		9.1.3	Beschrijven wat wordt verwacht van bedrijven en personen bij het werken met privacy gevoelige gegevens.

CATEGORIE	KENNISGEBIED	REF.	KENNISONDERWERP
	9.2 Inrichting	9.2.1	De werkzaamheden en bevoegdheden van de functionaris gegevensbewerking beschrijven.
		9.2.2	De verantwoordelijkheden van medewerkers en lijnmanagement bij het werken met persoonsgegevens benoemen.
		9.2.3	De rol van de autoriteit persoonsgegevens (AP) benoemen.
	9.3 Bewerking	9.3.1	De term bewerking beschrijven.
		9.3.2	De voorwaarden die in een bewerkingsovereenkomst moeten staan benoemen. Onder andere: rechten, plichten, exit strategie.
10 Betrokkenen	*10.1 Rechten en plichten*	10.1.1	De aspecten die voortvloeien uit de privacy wetgeving benoemen en beschrijven. Onder andere recht om vergeten te worden, portabiliteit, inzagerecht en correctie.
		10.1.2	Uitleggen wie bedoeld worden met ‘betrokkene’ en ‘verantwoordelijke’ met betrekking tot persoonsgegevens.
11 Wetgeving	*11.1 Datalekken*	11.1.1	Beschrijven wat een datalek is.
		11.1.2	De verschillende vormen van datalekken en de verschillen tussen die vormen beschrijven.
		11.1.3	Beschrijven hoe binnen een organisatie te handelen bij het ontstaan van een datalek.
		11.1.4	Benoemen wanneer en bij wie een datalek gemeld moet worden.