ECDL Core Syllabus 5
IT-Security

ECDL
Europäischer
Computer Führerschein

Modul 8 – IT-Security

Dieses Dokument beinhaltet den Syllabus für Modul 8, IT-Security, und stellt die Grundlage für den theoretischen Test über dieses Modul dar.

ZIELE MODUL 8

Das Modul IT-Security erfordert von den Kandidatinnen und Kandidaten grundlegende Kenntnisse über eine sichere Nutzung der IKT im Alltag, über geeignete Maßnahmen für eine sichere Verbindung zu einem Netzwerk, über Sicherheit im Internet und über die richtige Handhabung von Daten und Informationen – mit dem Ziel, die IKT sicher anwenden zu können und sicherheitsspezifischen Herausforderungen der IKT gewachsen zu sein.

Die Kandidatinnen und Kandidaten müssen

- verstehen, wie wichtig die Sicherheit von Daten, Informationen und Geräten ist, und die Bedeutung von Privatsphäre und Identitätsdiebstahl kennen
- Computer, Geräte und Netzwerke vor Malware und unberechtigtem Zugriff schützen können
- Netzwerktypen und Verbindungsarten kennen und über netzwerkspezifische Themen wie zB Firewalls Bescheid wissen
- das World Wide Web sicher nutzen und im Internet sicher kommunizieren können
- sicherheitsrelevante Aspekte bei der Kommunikation, zB per E-Mail oder Instant Messaging, verstehen
- Daten sichern und wiederherstellen können; über eine sichere Aufbewahrung von Daten und Geräten Bescheid wissen

Österreichische Computer Gesellschaft (OCG), Hintere Zollamtsstraße 1, 1030 Wien, Tel.: +43 1 512 02 35-0
www.ocg.at, www.ecdl.at

Kategorie	Wissensgebiet	Ref.	Fertigkeit
8.1 Grundbegriffe zu Sicherheit	8.1.1 Datenbedrohung	8.1.1.1	Zwischen Daten und Informationen unterscheiden können
		8.1.1.2	Den Begriff Cybercrime (Internetkriminalität) verstehen
		8.1.1.3	Den Unterschied zwischen Hacking, Cracking und ethischem Hacking verstehen
		8.1.1.4	Bedrohung für Daten durch höhere Gewalt kennen, wie: Feuer, Hochwasser, Krieg, Erdbeben
		8.1.1.5	Bedrohung für Daten durch MitarbeiterInnen, Dienstleister und andere externe Personen kennen
	8.1.2 Wert von Informationen	8.1.2.1	Verstehen, weshalb personenbezogene Daten zu schützen sind, zB um Identitätsdiebstahl und Betrug zu verhindern

Kategorie	Wissensgebiet	Ref.	Fertigkeit
		8.1.2.2	Verstehen, weshalb sensible Firmendaten zu schützen sind, zB um den Diebstahl oder Missbrauch von Kundendaten oder Finanzdaten zu verhindern
		8.1.2.3	Maßnahmen kennen, um unberechtigten Zugriff auf Daten zu verhindern, wie: Verschlüsselung, Passwörter
		8.1.2.4	Grundlegende Merkmale von Datensicherheit verstehen, wie: Vertraulichkeit, Integrität, Verfügbarkeit
		8.1.2.5	Wesentliche rechtliche Grundlagen für Datenschutz und Datenhaltung im eigenen Land kennen
		8.1.2.6	Verstehen, weshalb die Erstellung und die Einhaltung von Sicherheitsstrategien und Richtlinien für die Nutzung von IKT wichtig sind
	8.1.3 Persönliche Sicherheit	8.1.3.1	Den Begriff Social Engineering verstehen und die Ziele von Social Engineering kennen, wie: Informationen sammeln, Betrug, Zugriff auf Computer
		8.1.3.2	Methoden des Social Engineering kennen, wie: Telefonanrufe, Phishing, Shoulder Surfing
		8.1.3.3	Den Begriff Identitätsdiebstahl verstehen und die Folgen von Identitätsmissbrauch in persönlicher, finanzieller, geschäftlicher und rechtlicher Hinsicht kennen
		8.1.3.4	Methoden des Identitätsdiebstahls kennen, wie: Information Diving, Skimming, Pretexting
	8.1.4 Sicherheit für Dateien	8.1.4.1	Die Auswirkung von aktivierten und deaktivierten Makro-Sicherheitseinstellungen verstehen
		8.1.4.2	Mit einem Passwort Dateien schützen, zB: Dokumente, komprimierte Dateien, Tabellenkalkulationsdateien
		8.1.4.3	Die Vorteile und die Grenzen von Verschlüsselung verstehen
8.2 Malware	8.2.1 Definition und Funktionsweise	8.2.1.1	Den Begriff Malware verstehen
		8.2.1.2	Verschiedene Möglichkeiten zum Verbergen von Malware kennen, wie: Rootkit, Backdoor-Trojaner
	8.2.2 Typen	8.2.2.1	Typen von sich selbst verbreitender Malware kennen und ihre Funktionsweise verstehen, wie: Virus, Wurm
		8.2.2.2	Malware kennen für Datendiebstahl, Betrug oder Erpressung und die Funktionsweise dieser Malware verstehen, wie: Adware, Spyware, Botnet, Keylogger und Dialer
	8.2.3 Schutz	8.2.3.1	Die Funktionsweise und die Grenzen von Antiviren-Software verstehen
		8.2.3.2	Laufwerke, Ordner und Dateien mit Antiviren-Software scannen; Scans mit Antiviren-Software planen
		8.2.3.3	Den Begriff Quarantäne verstehen und die Auswirkung der Quarantäne auf infizierte oder verdächtige Dateien kennen
		8.2.3.4	Verstehen, weshalb es wichtig ist, Software-Updates zu installieren und Virensignaturen zu aktualisieren

Kategorie	Wissensgebiet	Ref.	Fertigkeit
8.3 Sicherheit im Netzwerk	8.3.1 Netzwerke	8.3.1.1	Den Begriff Netzwerk verstehen und Netzwerktypen kennen, wie: Local Area Network (LAN), Wide Area Network (WAN), Virtual Private Network (VPN)
		8.3.1.2	Die Aufgaben der Netzwerk-Administration verstehen, wie: Authentifizierung, Benutzerrechte verwalten, Nutzung dokumentieren
		8.3.1.3	Die Funktion und die Grenzen einer Firewall kennen
	8.3.2 Netzwerk-verbindungen	8.3.2.1	Möglichkeiten zur Verbindung mit einem Netzwerk kennen, wie: Leitungskabel, drahtlose Verbindung
		8.3.2.2	Verstehen, wodurch sich eine Verbindung zu einem Netzwerk auf die Datensicherheit auswirken kann, wie: Malware, unberechtigter Zugriff auf Daten, Schutz der Privatsphäre
	8.3.3 Sicherheit im drahtlosen Netz	8.3.3.1	Verstehen, dass es wichtig ist, den Zugriff auf drahtlose Netze mit einem Passwort zu schützen
		8.3.3.2	Verschiedene Verfahren zum Schutz von drahtlosen Netzwerken kennen, wie: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC)
		8.3.3.3	Sich bewusst sein, dass ein ungeschütztes drahtloses Netzwerk Eindringlingen den drahtlosen Zugriff auf Daten ermöglicht
		8.3.3.4	Eine Verbindung zu einem geschützten/nicht geschützten drahtlosen Netzwerk herstellen
	8.3.4 Zugriffskontrolle	8.3.4.1	Verstehen, wozu ein Netzwerkzugang dient und weshalb ein Zugriff mittels Benutzername und Passwort erfolgen soll
		8.3.4.2	Richtlinien für ein gutes Passwort kennen, wie: geheim halten, regelmäßig ändern; aus Buchstaben, Ziffern und Sonderzeichen zusammensetzen; angemessene Mindestlänge beachten
		8.3.4.3	Biometrische Verfahren zur Zugangskontrolle kennen, wie: Fingerabdruck scannen, Auge scannen
8.4 Sichere Web-Nutzung	8.4.1 Browser verwenden	8.4.1.1	Sich bewusst sein, dass bestimmte Online-Aktivitäten (Einkaufen, E-Banking) nur auf sicheren Webseiten erfolgen sollten
		8.4.1.2	Merkmale einer sicheren Website kennen, wie: https, Schloss-Symbol
		8.4.1.3	Sich der Gefahren durch Pharming bewusst sein
		8.4.1.4	Den Begriff Digitales Zertifikat verstehen; die Gültigkeit eines Digitalen Zertifikats überprüfen können
		8.4.1.5	Den Begriff Einmal-Kennwort verstehen
		8.4.1.6	Einstellungen zu Formulardaten aktivieren/deaktivieren können, wie: AutoVervollständigen, Speichern
		8.4.1.7	Den Begriff Cookie verstehen
		8.4.1.8	Einstellungen vornehmen, um Cookies zuzulassen oder nicht zuzulassen
		8.4.1.9	In einem Browser eigene Daten löschen, wie: Verlauf, temporäre Internetdateien, Passwörter, Cookies, Formulardaten
		8.4.1.10	Den Zweck, die Funktionsweise und die Arten von Software zur Inhaltskontrolle kennen, wie: Filter, Kindersicherung

Kategorie	Wissensgebiet	Ref.	Fertigkeit
	8.4.2 Soziale Netzwerke	8.4.2.1	Verstehen, dass es wichtig ist, vertrauliche Informationen nicht in sozialen Netzwerken zu veröffentlichen
		8.4.2.2	Sich der Notwendigkeit bewusst sein, in sozialen Netzwerken die Einstellungen zum Schutz der Privatsphäre anzuwenden
		8.4.2.3	Mögliche Gefahren bei der Nutzung von sozialen Netzwerken kennen, wie: Cyber-Mobbing, Cyber-Grooming, irreführende oder gefährliche Information, falsche Identität, arglistige Links oder Nachrichten
8.5 Kommunikation	8.5.1 E-Mail	8.5.1.1	Verstehen, weshalb eine E-Mail verschlüsselt und entschlüsselt wird
		8.5.1.2	Den Begriff Digitale Signatur verstehen
		8.5.1.3	Wissen, wie eine digitale Signatur erstellt und hinzugefügt wird
		8.5.1.4	Sich der Möglichkeit bewusst sein, arglistige und unerwünschte E-Mails zu erhalten
		8.5.1.5	Den Begriff Phishing verstehen; typische Merkmale von Phishing kennen, wie: Verwendung der Namen von seriösen Unternehmen und Personen, Links zu gefälschten Webseiten
		8.5.1.6	Sich der Gefahr bewusst sein, dass ein Computer mit Malware infiziert werden kann: beim Öffnen eines Attachments, das ein Makro enthält; beim Öffnen einer ausführbaren Datei
	8.5.2 Instant Messaging	8.5.2.1	Den Begriff Instant Messaging (IM) verstehen und die Einsatzgebiete von IM kennen
		8.5.2.2	Schwachstellen bei der Sicherheit von IM verstehen und Gefahren kennen, wie: Malware, Backdoor-Zugang, Zugriff auf Dateien
		8.5.2.3	Methoden kennen, um beim Gebrauch von IM Vertraulichkeit sicherzustellen, wie: Verschlüsselung, Nicht-Veröffentlichung von wichtigen Informationen, Zugriff auf Daten einschränken
8.6 Sicheres Daten-Management	8.6.1 Daten sichern und Backups erstellen	8.6.1.1	Maßnahmen zur physischen Sicherung von Geräten kennen, wie: Geräte inventarisieren, Sicherungskabel, Zugangskontrolle
		8.6.1.2	Wissen, wie wichtig eine Sicherungskopie (Backup) für den Fall des Verlusts von Daten ist, zB von: Firmen-Datenbanken, Finanzbuchhaltung, Favoriten/Lesezeichen
		8.6.1.3	Wesentliche Merkmale eines Konzepts zur Datensicherung kennen, wie: Regelmäßigkeit, Häufigkeit, Ablaufplanung, Speicherort
		8.6.1.4	Backup erstellen
		8.6.1.5	Daten wiederherstellen und überprüfen
	8.6.2 Sichere Datenvernichtung	8.6.2.1	Den Sinn und Zweck einer endgültigen Vernichtung von Daten auf Laufwerken oder in Geräten verstehen
		8.6.2.2	Den Unterschied zwischen der Löschung von Daten und der endgültigen Vernichtung von Daten kennen
		8.6.2.3	Methoden zur endgültigen Vernichtung von Daten kennen, wie: Datenträger schreddern, physisch zerstören, entmagnetisieren; Software zur Datenvernichtung anwenden