ICDL
The Digital Skills Standard

OESTERREICHISCHE COMPUTER GESELLSCHAFT ®
AUSTRIAN COMPUTER SOCIETY

IT-SECURITY

Sicherheit im Internet und Datenschutz

icdl.org

Zweck dieses Dokuments

Dieses Dokument listet die Lerninhalte für das ICDL Modul ***IT-Security*** Version 3.0 auf und beschreibt, welche Fertigkeiten von den Absolvent*innen des Moduls erwartet werden. Die theoretischen und praktischen Aufgaben der Tests zu diesem Modul beruhen auf den Inhalten dieses Lernzielkatalogs. Approbierte Lernmaterialien decken dessen Inhalte ab.

Der ICDL ist eine Initiative der ICDL Foundation und wird in Österreich von der OCG betreut.

ICDL Foundation

The Chase, Arkle Road, Level 1
Sandyfod
Co. Dublin
D18 Y3X2
Republic of Ireland
Web: www.icdl.org

Österreichische Computer Gesellschaft (OCG)

Wollzeile 1
A-1010 Wien
Tel: +43 1 512 02 35-0
E-Mail: info@ocg.at
Web: www.ocg.at

Hinweis

Die aktuelle deutschsprachige Version von ICDL Lernzielkatalogen für Österreich ist auf der ICDL Website www.icdl.at veröffentlicht.

Haftung

Die OCG hat dieses Dokument mit Sorgfalt erstellt, kann aber weder Richtigkeit und Vollständigkeit der enthaltenen Informationen zusichern noch Haftung für durch diese Informationen verursachte Schäden übernehmen.

Urheberrecht

IT-SECURITY

Dieses Modul vermittelt Kenntnisse für eine sichere Nutzung der IKT im Alltag, über geeignete Maßnahmen für eine sichere Netzwerkverbindung, über Sicherheit im Internet und über die richtige Handhabung von Daten und Informationen.

LERNZIELE

Absolvent*innen dieses Moduls können

- verstehen, wie wichtig die Sicherheit von Daten und Informationen ist und die Grundsätze zum Datenschutz, zur Datenspeicherung, zur Datenkontrolle und zum Schutz der Privatsphäre kennen,
- Bedrohungen für die persönliche Sicherheit durch Social Engineering, Künstliche Intelligenz (KI) und Identitätsdiebstahl erkennen sowie die mögliche Gefährdung von Daten durch Cloud Computing kennen,
- Passwörter und Verschlüsselung zur Sicherung von Dateien und Daten einsetzen,
- die Bedrohung durch Malware, einschließlich KI-Malware, verstehen und Computer, mobile Geräte und Netzwerk vor Malware schützen sowie auf Malware-Attacken richtig reagieren,
- übliche Sicherheitsmerkmale von Netzwerken und Drahtlosverbindungen und deren Risiken kennen und Personal Firewalls sowie persönliche Hotspots nutzen,
- Sicherheitsrisiken, die mit der Nutzung von mobilen Geräten, Wearables und IoT (Internet of Things) Geräten verbunden sind verstehen und sie sicher verwenden,
- Daten vor unbefugtem Zugriff schützen; Passwörter sicher verwalten und aktualisieren,
- geeignete Webbrowser-Einstellungen verwenden, die Vertrauenswürdigkeit einer Website feststellen, sicher im Internet surfen und den privaten Browser-Modus nutzen,
- verstehen, dass Sicherheitsprobleme bei der Kommunikation per E-Mail, VoIP (Voice over IP), Instant Messaging, in Sozialen Netzwerken sowie durch die Nutzung mobiler Geräte auftreten können,
- Daten auf lokalen und externen Speicherorten und in der Cloud sichern und wiederherstellen sowie Daten und Geräte sicher löschen und entsorgen.

1. GRUNDBEGRIFFE ZUR SICHERHEIT

1.1. Datenbedrohung

1.1.1 Zwischen Daten und Informationen unterscheiden können.

1.1.2 Die Begriffe Cybersicherheit, Cyberangriff, Cyberkriminalität, Hacking und Cyberkrieg verstehen.

1.1.3 Böswillige und unabsichtliche Bedrohung für Daten durch Einzelpersonen, Dienstleister und externe Organisationen kennen.

1.1.4 Bedrohung für Daten durch höhere Gewalt kennen, wie: Feuer, Hochwasser, Krieg, Erdbeben.

1.1.5 Bedrohung für Daten durch die Verwendung von Cloud-Computing kennen, wie: Datenkontrolle, möglicher Verlust der Privatsphäre.

1.2. Wert von Information

1.2.1 Grundlegende Merkmale von Datensicherheit verstehen, wie: Vertraulichkeit, Integrität, Verfügbarkeit.

1.2.2 Verstehen, weshalb personenbezogene Daten zu schützen sind, z. B. um Identitätsdiebstahl und Betrug zu verhindern, zum Schutz der Privatsphäre.

1.2.3 Verstehen, weshalb Firmendaten auf Computern und mobilen Geräten zu schützen sind, z. B. um Diebstahl, betrügerische Verwendung, unabsichtlichen Datenverlust und Sabotage zu verhindern.

1.2.4 Allgemeine Grundsätze für Datenschutz/Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle kennen, wie: Transparenz, Notwendigkeit, Verhältnismäßigkeit.

1.2.5 Die Begriffe Betroffene und Auftraggeber verstehen. Verstehen, wie die Grundsätze für Datenschutz/ Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle für Betroffene und Auftraggeber angewendet werden.

1.2.6 Verstehen, dass bei der Nutzung von IKT die Einhaltung von Grundsätzen und Richtlinien wichtig ist; wissen, wie die Richtlinien üblicherweise bekanntgemacht werden bzw. zugänglich sind. Wissen, dass bei der Verarbeitung personenbezogene Daten lokale Gesetze zu Anwendung kommen.

1.3. Persönliche Sicherheit

1.3.1 Den Begriff Social Engineering verstehen und die Ziele kennen, wie: Umgehung von Sicherheitsmaßnahmen, Informationsdiebstahl, unerlaubtes Sammeln von Informationen, Betrug.

1.3.2 Methoden des Social Engineering kennen, wie: Telefonanrufe, Phishing, (inkl. Voice Phishing, QR Code Phishing, Wasserloch-Phishing), Pharming, Shoulder Surfing, Nachahmungsangriff (Impersonation), Tailgating (unbefugter Zugang), Baiting (Köder Angriff), Fake News, Deepfakes, durch Künstliche Intelligenz (KI) unterstützter Nachahmungsangriff.

1.3.3. Wissen, wie wichtig es ist als Schutz vor Social Engineering die Authentizität von digitalen Inhalten und digitaler Kommunikation, wie Webseiten, E-Mail, Social Media, Messaging Apps, QR Codes, Links und andern Kommunikationsformen festzustellen.

1.3.4 Den Begriff Identitätsdiebstahl verstehen und die Folgen von Identitätsmissbrauch in persönlicher, finanzieller, geschäftlicher und rechtlicher Hinsicht kennen.

1.3.5 Methoden des Identitätsdiebstahls kennen, wie: Information Diving, Skimming (illegales Auslesen von Bankkarten), Pretexting, Web Scraping (illegales Datenschürfen).

1.4. Sicherheit der Dateien

1.4.1 Die Auswirkung von aktivierten und deaktivierten Makro-Sicherheitseinstellungen verstehen.

1.4.2 Die Grundlagen von Datei- bzw. Geräte-Verschlüsselung verstehen und ihren Nutzen für die Sicherheit kennen. Wissen, wie wichtig es ist, das Passwort, den Schlüssel und das Zertifikat der Verschlüsselung nicht offenzulegen und nicht zu verlieren.

1.4.3 Eine Datei, einen Ordner oder ein Laufwerk verschlüsseln.

1.4.4 Dateien mit einem Passwort schützen, z. B.: Dokumente, Tabellen kalkulationsdateien, komprimierte Dateien.

2. MALWARE (SCHADSOFTWARE)

2.1. Arten und Funktionsweisen

2.1.1 Den Begriff Malware verstehen; verschiedene Arten von Malware kennen: Adware, Fileless Malware, Virus, Wurm, Trojaner, Bots, Ransomware, Spyware, Keylogging, Cryptojacking.

2.1.2. Wissen, wie sich KI (Künstliche Intelligenz) Malware von traditioneller Malware durch Fähigkeiten wie Anpassung, Lernen und Umgehung unterscheidet.

2.1.3 Arten von sich selbst verbreitender Malware kennen und ihre Funktionsweise verstehen, wie: Virus, Wurm.

2.1.4 Arten von Malware und ihre Funktionsweise für Datendiebstahl, Betrug oder Erpressung kennen, wie: Adware, Ransomware, Spyware, Bots, Keylogger.

2.2. Schutz

2.2.1 Verstehen, dass Antiviren-Software und Anti-Malware-Software auf Computern und mobilen Geräten installiert sein soll; ihre Funktionsweise und Grenzen verstehen.

2.2.2 Die Bedeutung von regelmäßigen Software-Updates für Antiviren-Software, Anti-Malware-Software, Web-Browser, Plug-ins, Anwendungsprogramme, Betriebssysteme verstehen.

2.2.3 Laufwerke, Ordner und Dateien mit Antiviren-Software und Anti-Malware-Software scannen; Zeitplan für Scans mit Antiviren-Software festlegen.

2.2.4 Verstehen, dass die Verwendung veralteter, unerwünschter und nicht mehr unterstützter Software mit Risiken verbunden ist, wie: zunehmende Gefährdung durch Malware, Inkompatibilität.

2.2.5. Den Begriff Quarantäne verstehen und die Auswirkung auf infizierte oder verdächtige Dateien kennen.

3. SICHERHEIT VON GERÄTEN UND NETZWERKEN

3.1. Netzwerke und Verbindungen

3.1.1 Den Begriff Netzwerk verstehen und übliche Netzwerktypen kennen, wie: Cloud Netzwerk, hybrides Netzwerk, Local Area Network (LAN), Wireless Local Area Network (WLAN), Wide Area Network (WAN), Virtual Private Network (VPN).

3.1.2 Verstehen, wodurch sich eine Verbindung zu einem Netzwerk auf die Sicherheit auswirken kann, wie: Malware, unberechtigter Zugriff auf Daten, Bedrohung der Privatsphäre.

3.1.3 Die Aufgaben der Netzwerk-Administration verstehen, wie: Authentifizierung, Benutzerrechte verwalten, Nutzung dokumentieren, sicherheitsrelevante Patches und Updates überwachen und installieren, Netzwerkverkehr überwachen, Malware im Netzwerk bekämpfen.

3.1.4 Die Funktion und die Grenzen einer Firewall bei der privaten Computernutzung und in einer Arbeitsumgebung verstehen.

3.1.5 Personal Firewall ein- und ausschalten; den durch die Personal Firewall laufenden Datenverkehr für eine Anwendung, einen Dienst/Funktion zulassen bzw. blockieren.

3.2. Sicherheit im drahtlosen Netz

3.2.1 Wissen, dass es wichtig ist drahtlose Verbindungen zu schützen und verschiedene Möglichkeiten zum Schutz von drahtlosen Netzwerken, deren Versionen und deren Grenzen kennen, wie: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA)/Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC) Filter, Service Set Identifier (SSID) verbergen.

3.2.2 Sich bewusst sein, dass auf ein ungeschütztes drahtloses Netzwerk Angriffe erfolgen können, wie: unbefugter Zugriff durch Eindringlinge, Hijacking, Man-in-the-Middle-Angriff.

3.2.3 Den Begriff Persönlicher Hotspot und die damit verbundenen Sicherheitsrisiken verstehen

3.2.4 Einen sicheren persönlichen Hotspot einschalten und ausschalten; Geräte sicher damit verbinden und trennen.

3.3. Geräte- und IoT Sicherheit

3.3.1 . Die Sicherheitsrisiken verstehen, die mit der Nutzung von mobilen Geräten, Wearables und IoT (Internet of Things) Geräten verbunden sind, wie: Geräte-Hijacking, Botnets, Lauschangriff und Überwachung, Datenschutzverletzungen, unautorisierter Zugriff

3.3.2 Maßnahmen zum Schutz von mobilen Geräten, Wearables und IoT Geräten kennen, wie: Software-Updates, Firmware-Updates, Zugriffskontrollen anwenden, sichere Verbindungen nützen, voreingestellte Standardpasswörter ändern, nicht benötigte Funktionen ausschalten.

4. ZUGRIFFSKONTROLLE

4.1. Methoden

4.1.1 Maßnahmen kennen, um unberechtigten Zugriff auf Daten zu verhindern, durch etwas, das Sie wissen, wie: Benutzername, Passwort, PIN, Verschlüsselung, Multi-Faktor-Authentifizierung.

4.1.2 Maßnahmen kennen, um unberechtigten Zugriff auf Daten zu verhindern, durch etwas, das Sie haben, wie: Sicherheitstoken, Smartcard, Smartphone; Vorteile und Grenzen der Maßnahmen kennen.

4.1.3 Maßnahmen kennen, um unberechtigten Zugriff auf Daten zu verhindern, indem Sie etwas verwenden wird, das Sie sind (biometrisches Verfahren), wie: Fingerabdruck, Auge scannen, Gesichtserkennung, Handgeometrie; Vorteile und Grenzen der Maßnahmen kennen.

4.1.4 Das Konzept und die Wichtigkeit von Multi-Faktor-Authentifizierung verstehen, um unberechtigten Zugriff auf Daten zu verhindern.

4.1.5 Den Begriff und die Wichtigkeit von Passkeys kennen, um unberechtigten Zugriff auf Daten zu verhindern.

4.1.6. Verstehen, wozu ein Netzwerk-Konto dient.

4.1.7. Verstehen, dass der Zugang zu einem Netzwerk-Konto mit Benutzername und Passwort erfolgen soll, und dass der Konto-Zugang gesperrt oder abgemeldet werden sollte, wenn er nicht genutzt wird.

4.2. Passwort-Verwaltung

4.2.1 Richtlinien für ein gutes Passwort kennen, wie: angemessene Mindestlänge beachten, aus Buchstaben und Ziffern und Sonderzeichen zusammensetzen, geheim halten, regelmäßig ändern, unterschiedliche Passwörter für unterschiedliche Dienste.

4.2.2 Die Funktion und die Grenzen einer Passwort-Verwaltungssoftware verstehen sowie die Risiken von Cloud-basierter und lokal installierter Passwort-Verwaltungssoftware kennen.

5. SICHERE WEB-NUTZUNG

5.1. Browser-Einstellungen

5.1.1 Einstellungen zum Ausfüllen von Formularen aktivieren und deaktivieren, wie: automatische Vervollständigung, automatisches Speichern.

5.1.2 In einem Browser persönliche Daten löschen, wie: Browserverlauf, Downloadverlauf, temporäre Internetdateien, Passwörter, Cookies, Formulardaten.

5.2. Sicheres Surfen

5.2.1 Sich bewusst sein, dass bestimmte Online-Aktivitäten (Einkaufen, E-Banking, E-Health) nur auf sicheren Webseiten über eine gesicherte Netzwerkverbindung erfolgen sollen.

5.2.2 Kriterien zur Beurteilung der Vertrauenswürdigkeit einer Website kennen, wie: inhaltliche Qualität, Aktualität, gültige URL, Information zum Inhaber der Webseite (Impressum), Kontaktdaten, Sicherheitszertifikat, Überprüfung der Domain-Inhaberschaft.

5.2.3 Die möglichen Gefahren von unsicheren Internet-Verbindungen kennen, wie: Abfangen von Kommunikation, gefälschte Webseiten, Injection-Angriffe.

5.2.4 Den Zweck und die Funktionsweise von Software zur Inhaltskontrolle kennen, wie: Internet-Filterprogramme, Kinderschutz-Software.

5.2.5. Die Vorteile von privatem Browser-Modus (Inkognito-Modus) kennen. Ein privates Bowserfenster öffnen.

6. KOMMUNIKATION

6.1. E-Mail

6.1.1 Verstehen, weshalb eine E-Mail verschlüsselt und entschlüsselt wird.

6.1.2 Wissen, welchen Zweck das digitale Signieren von E-Mails hat.

6.1.3 Typische Merkmale von Phishing, Malware, Spam-E-Mails kennen, wie: Spoofing (Identitätsverschleierung), Verwendung der Namen von seriösen Unternehmen und Personen, Verwendung von Logos und Markenzeichen, Links zu gefälschten Webseiten, Aufforderung zur Bekanntgabe persönlicher Daten, verdächtige E-Mail-Anhänge.

6.1.4 Wissen, dass Phishing-Attacken den betroffenen seriösen Unternehmen und zuständigen Behörden/Organisationen, E-Mail-Anbietern gemeldet werden können.

6.1.5 Sich der Gefahr bewusst sein, dass ein Computer oder mobiles Gerät mit Malware infiziert werden kann, wenn ein E-Mail-Attachment geöffnet wird, das ein Makro oder eine ausführbare Datei enthält.

6.2. Soziale Netzwerke

6.2.1 Verstehen, dass es wichtig ist, vertrauliche oder personenbezogene Informationen nicht in sozialen Netzwerken zu veröffentlichen.

6.2.2 Sich der Notwendigkeit bewusst sein, in sozialen Netzwerken geeignete Konto-Einstellungen auszuwählen und regelmäßig zu überprüfen, wie: Privatsphäre, Standort; Regeln, wer gepostete Inhalte sehen darf.

6.2.3 Wissen, dass es wichtig ist Online-Konten stillzulegen und alle damit verbunden Daten zu löschen, sobald sie nicht mehr länger aktiv genutzt werden.

6.2.4 Online-Konto und Online-Daten in sozialen Netzwerken löschen.

6.2.5 Mögliche Gefahren bei der Nutzung von sozialen Netzwerken kennen, wie: Cyber-Mobbing, Cyber-Grooming, bösartige Veröffentlichung persönlicher Inhalte, falsche Identitäten; betrügerische oder arglistige Links, Inhalte oder Nachrichten; falsche oder irreführende Inhalte; Fake News.

6.2.6 Wissen, dass missbräuchliche Verwendung oder Fehlverhalten in sozialen Netzwerken dem jeweiligen Service-Provider und zuständigen Behörden/Organisationen gemeldet werden kann.

6.3. VoIP, Instant Massaging und Mobile Geräte

6.3.1 Schwachstellen bei der Sicherheit von Instant Messaging (IM) und Voice over Internet Protocol (VoIP) verstehen und Gefahren kennen, wie: Malware, Backdoor-Zugang, Zugriff auf Dateien, Lauschangriff.

6.3.2 Sicherheitsrisiken bei der Nutzung von GPS und Bluetooth auf mobilen Geräten kennen, wie: Standortverfolgung, Spoofing, Verlust der Privatsphäre, unberechtigter Zugriff.

6.3.3. Sicherheitsrisiken bei der Nutzung von NFC (Near Field Communication) auf mobilen Geräten kennen, wie: Lauschangriff, Datenbeschädigung oder -verfälschung, Relay-Angriffe, unberechtigte Transaktionen.

6.3.4 Verstehen, welche Folgen die Verwendung von Anwendungen aus inoffiziellen App-Stores haben kann, wie: mobile Malware, unnötiger Ressourcenverbrauch, Zugriff auf persönliche Daten, schlechte Qualität, versteckte Kosten.

6.3.5 Wissen, welche Einstellungen und App-Berechtigungen es bei mobilen Anwendungen gibt; wissen, dass mobile Applikationen private Informationen von mobilen Geräten auslesen können, wie: Kontaktdaten, Standortverlauf, Bilder.

6.3.6 Für den Fall, dass ein mobiles Gerät abhandenkommt, Sofortmaßnahmen und Vorsichtsmaßnahmen kennen, wie: Fernsperrung, Fernlöschung, Geräteortung.

7 SICHERE DATENVERWALTUNG

7.1. Daten sichern und Backups erstellen

7.1.1 Maßnahmen zur physischen Sicherung von Computern und mobilen Geräten kennen, wie: nicht unbeaufsichtigt lassen, Standort der Geräte und weitere Details aufzeichnen, Sicherungskabel verwenden, Zugangskontrolle.

7.1.2 Wissen, wie wichtig eine Sicherungskopie für den Fall des Datenverlusts auf Computern und anderen Geräten ist.

7.1.3 Wesentliche Merkmale eines Konzepts zur Datensicherung kennen, wie: Regelmäßigkeit/Häufigkeit, Zeitplan, Ablageort, Datenkompression.

7.1.4 Mögliche Gefahren beim Backup von Daten auf bestimmte Orte kennen, wie: lokales Laufwerk, externes Laufwerk/Datenträger, Cloud-Speicher; 3-2-1 Backup-Regel kennen.

7.1.5 Backup an einem Speicherort erstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.

7.1.6 Daten von einem Backup-Speicherort wiederherstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.

7.2. Daten sicher löschen und vernichten

7.2.1 Den Unterschied zwischen der Löschung von Daten und der endgültigen Löschung/Vernichtung von Daten kennen.

7.2.2 Den Sinn und Zweck einer endgültigen Löschung/Vernichtung von Daten auf Laufwerken oder Geräten verstehen.

7.2.3 Sich bewusst sein, dass das Löschen von Inhalten bei manchen Diensten nicht endgültig ist, wie: Soziale Netzwerke, Blogs, Internetforen, Cloud-Dienste.

7.2.4 Methoden zur endgültigen Datenvernichtung kennen, wie: Laufwerke/Datenträger zerstören, z. B. Schreddern; Entmagnetisierung; Software zur Datenvernichtung verwenden.

Platz für Notizen:

ICDL ZERTIFIKATE

ICDL BASE (UMFASST 4 MODULE)

- Computer Grundlagen
- Online Grundlagen
- Textverarbeitung
- Tabellenkalkulation

ICDL STANDARD (UMFASST 7 MODULE)

4 BASE MODULE

- Computer-Grundlagen
- Online Grundlagen
- Textverarbeitung
- Tabellenkalkulation

+ 3 WAHLMODULE

- Präsentation
- IT-Security
- Online Zusammenarbeit
- Datenbanken anwenden
- Bildbearbeitung*
- Computing*
- Künstliche Intelligenz*

ICDL ADVANCED EXPERT (UMFASST 4 MODULE)

- Textverarbeitung Advanced*
- Tabellenkalkulation Advanced*
- Präsentation Advanced*
- Datenbank Advanced*

EINZELZERTIFIKAT

- Robotik*

* Modul auch als Einzelzertifikat verfügbar

ICDL
The Digital Skills Standard

Österreichische Computer Gesellschaft (OCG) | Wollzeile 1 | 1010 Wien
+43 1 512 02 35 - 0 | info@ocg.at | ocg.at | icdl.at