



INHALT

Der Aufbau dieser Lernunterlage ist der Gliederung des ICDL-Lernzielkatalog 3.0 angepasst. Kapitel und Unterkapitel sind daher in der gleichen Nummerierung, wie sie im ICDL-Lernzielkatalog verwendet wird.

1	GRUNDBEGRIFFE ZU SICHERHEIT	9
1.1	Datenbedrohung.....	9
1.1.1	Zwischen Daten und Informationen unterscheiden können.....	9
1.1.2	Die Begriffe Cybersicherheit, Cyberangriff, Cybercrime, Hacking und Cyberkrieg verstehen.....	10
1.1.3	Böswillige und unabsichtliche Bedrohung für Daten durch Einzelpersonen, Dienstleister und externe Organisationen kennen.....	12
1.1.4	Bedrohung für Daten durch höhere Gewalt kennen, wie: Feuer, Hochwasser, Krieg, Erdbeben	13
1.1.5	Bedrohung für Daten durch die Verwendung von Cloud-Computing kennen, wie: Datenkontrolle, möglicher Verlust der Privatsphäre	14
1.2	Wert von Informationen	15
1.2.1	Grundlegende Merkmale von Datensicherheit verstehen, wie: Vertraulichkeit, Integrität, Verfügbarkeit	16
1.2.2	Verstehen, weshalb personenbezogene Daten zu schützen sind, zB um Identitätsdiebstahl und Betrug zu verhindern, zum Schutz der Privatsphäre	17
1.2.3	Verstehen, weshalb Firmendaten auf Computern und mobilen Geräten zu schützen sind, zB um Diebstahl, betrügerische Verwendung, unabsichtlichen Datenverlust und Sabotage zu verhindern.....	17
1.2.4	Allgemeine Grundsätze für Datenschutz/Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle kennen, wie: Transparenz, Notwendigkeit, Verhältnismäßigkeit	18
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	19
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.....	20
1.3	Persönliche Sicherheit	21
1.3.1	Den Begriff Social Engineering verstehen und die Ziele kennen, wie: Umgehung von Sicherheitsmaßnahmen, Informationsdiebstahl, unerlaubtes Sammeln von Informationen, Betrug	21
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.....	22
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	25
1.3.4	Den Begriff Identitätsdiebstahl verstehen und die Folgen von Identitätsmissbrauch in persönlicher, finanzieller, geschäftlicher und rechtlicher Hinsicht kennen	26
1.3.5	Methoden des Identitätsdiebstahls kennen, wie: Information Diving, Skimming (illegales Auslesen von Bankkarten), Pretexting, Web Scraping (illegales Datenschürfen).....	27
1.4	Sicherheit der Dateien.....	28
1.4.1	Die Auswirkung von aktivierten und deaktivierten Makro-Sicherheitseinstellungen verstehen.....	28
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.....	29
1.4.3	Eine Datei, einen Ordner oder ein Laufwerk verschlüsseln.....	30
1.4.4	Dateien mit einem Passwort schützen, zB: Dokumente, Tabellenkalkulationsdateien, komprimierte Dateien	35
2	MALWARE (SCHADSOFTWARE).....	39
2.1	Arten und Funktionsweisen.....	39
2.1.1	Den Begriff Malware verstehen; verschiedene Arten von Malware kennen: Adware, Fileless Malware, Virus, Wurm, Trojaner, Bots, Ransomware, Spyware, Keylogging, Cryptojacking	39
2.1.2	Wissen, wie sich KI (Künstliche Intelligenz) Malware von traditioneller Malware durch Fähigkeiten wie Anpassung, Lernen und Umgehung unterscheidet.....	41
2.1.3	Arten von sich selbst verbreitender Malware kennen und ihre Funktionsweise verstehen, wie: Virus, Wurm	42
2.1.4	Arten von Malware und ihre Funktionsweise für Datendiebstahl, Betrug oder Erpressung kennen, wie: Adware, Ransomware, Spyware, Bots, Keylogger	42
2.2	Schutz	45
2.2.1	Verstehen, dass Antiviren-Software und Anti-Malware-Software auf Computern und mobilen Geräten installiert sein soll; ihre Funktionsweise und Grenzen verstehen	45
2.2.2	Die Bedeutung von regelmäßigen Software-Updates für Antiviren-Software, Anti-Malware-Software, Web-Browser, Plug-ins, Anwendungsprogramme, Betriebssysteme verstehen.....	47
2.2.3	Laufwerke, Ordner und Dateien mit Antiviren-Software und Anti-Malware-Software scannen; Zeitplan für Scans mit Antiviren-Software festlegen	47



2.2.4	Verstehen, dass die Verwendung veralteter, unerwünschter und nicht mehr unterstützter Software mit Risiken verbunden ist, wie: zunehmende Gefährdung durch Malware, Inkompatibilität	49
2.2.5	Den Begriff Quarantäne verstehen und die Auswirkung auf infizierte oder verdächtige Dateien kennen.....	49
Wissens-Check		51
3	SICHERHEIT VON GERÄTEN UND NETZWERKEN	53
3.1	Netzwerke und Verbindungen.....	53
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)	53
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.....	54
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	55
3.1.4	Die Funktion und die Grenzen einer Firewall bei der privaten Computernutzung und in einer Arbeitsumgebung verstehen	56
3.1.5	Personal Firewall ein- und ausschalten; den durch die Personal Firewall laufenden Datenverkehr für eine Anwendung, einen Dienst/Funktion zulassen bzw. blockieren	57
3.2	Sicherheit im drahtlosen Netz.....	59
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), Media Access Control (MAC) Filter, Service Set Identifier (SSID) verbergen.....	59
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	61
3.2.3	Den Begriff Persönlicher Hotspot und die damit verbundenen Sicherheitsrisiken verstehen.....	63
3.2.4	Einen sicheren Persönlichen Hotspot einschalten und ausschalten; Geräte sicher damit verbinden und trennen	64
3.3	Geräte- und IoT Sicherheit.....	65
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	66



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.....	66
Wissens-Check.....		68
4	ZUGRIFFSKONTROLLE	69
4.1	Methoden	69
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.....	69
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.....	70
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.....	71
4.1.4	Das Konzept und die Wichtigkeit von Multi-Faktor-Authentifizierung verstehen, um unberechtigten Zugriff auf Daten zu verhindern.....	72
4.1.5	Den Begriff und die Wichtigkeit von Passkeys kennen, um unberechtigten Zugriff auf Daten zu verhindern	72
4.1.6	Verstehen, wozu ein Netzwerk-Konto dient.....	73
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	73
4.2	Passwort-Verwaltung	74
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.....	75
4.2.2	Die Funktion und die Grenzen einer Passwort-Verwaltungssoftware verstehen sowie die Risiken von Cloud-basierter und lokal installierter Passwort-Verwaltungssoftware kennen	76
5	SICHERE WEB-NUTZUNG	79
5.1	Browser-Einstellungen.....	79
5.1.1	Einstellungen zum Ausfüllen von Formularen aktivieren und deaktivieren, wie: automatische Vervollständigung, automatisches Speichern	80
5.1.2	In einem Browser persönliche Daten löschen, wie: Browserverlauf, Downloadverlauf, temporäre Internetdateien, Passwörter, Cookies, Formulardaten.....	80
5.2	Sicheres Surfen	82



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.....	82
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.....	83
5.2.3	Die möglichen Gefahren von unsicheren Internet-Verbindungen kennen, wie: Abfangen von Kommunikation, gefälschte Webseiten, Injection-Angriffe	84
5.2.4	Den Zweck und die Funktionsweise von Software zur Inhaltskontrolle kennen, wie: Internet-Filterprogramme, Kinderschutz-Software	85
5.2.5	Die Vorteile von privatem Browser-Modus (Inkognito-Modus) kennen. Ein privates Browserfenster öffnen.....	89
Wissens-Check		91
6	KOMMUNIKATION	93
6.1	E-Mail	93
6.1.1	Verstehen, weshalb eine E-Mail verschlüsselt und entschlüsselt wird	93
6.1.2	Wissen, welchen Zweck das digitale Signieren von E-Mails hat	95
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	96
6.1.4	Wissen, dass Phishing-Attacken den betroffenen seriösen Unternehmen und zuständigen Behörden/Organisationen, E-Mail-Anbietern gemeldet werden können.....	100
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.....	100
6.2	Soziale Netzwerke	102
6.2.1	Verstehen, dass es wichtig ist, vertrauliche oder personenbezogene Informationen nicht in sozialen Netzwerken zu veröffentlichen	102
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	102
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.....	104
6.2.4	Online-Konto und Online-Daten in sozialen Netzwerken löschen	104
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	105



6.2.6	Wissen, dass missbräuchliche Verwendung oder Fehlverhalten in sozialen Netzwerken dem jeweiligen Service-Provider und zuständigen Behörden/Organisationen gemeldet werden kann.....	106
6.3	VoIP, Instant Messaging und Mobile Geräte	108
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	108
6.3.2	Sicherheitsrisiken bei der Nutzung von GPS und Bluetooth auf mobilen Geräten kennen, wie: Standortverfolgung, Spoofing, Verlust der Privatsphäre, unberechtigter Zugriff.....	109
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	110
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.....	110
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.....	111
6.3.6	Für den Fall, dass ein mobiles Gerät abhandenkommt, Sofortmaßnahmen und Vorsichtsmaßnahmen kennen, wie: Fernsperrung, Fernlöschung, Geräteortung	113
	Wissens-Check.....	115
7	SICHERE DATEN-VERWALTUNG	117
7.1	Daten sichern und Backups erstellen	117
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.....	117
7.1.2	Wissen, wie wichtig eine Sicherungskopie für den Fall des Datenverlusts auf Computern und anderen Geräten ist.....	118
7.1.3	Wesentliche Merkmale eines Konzepts zur Datensicherung kennen, wie: Regelmäßigkeit/Häufigkeit, Zeitplan, Ablageort, Datenkompression	119
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.....	119
7.1.5	Backup an einem Speicherort erstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.....	121
7.1.6	Daten von einem Backup-Speicherort wiederherstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.....	123
7.2	Daten sicher löschen und vernichten	125



7.2.1	Den Unterschied zwischen der Löschung von Daten und der endgültigen Löschung/Vernichtung von Daten kennen	125
7.2.2	Den Sinn und Zweck einer endgültigen Löschung/Vernichtung von Daten auf Laufwerken oder Geräten verstehen	125
7.2.3	Sich bewusst sein, dass das Löschen von Inhalten bei manchen Diensten nicht endgültig ist, wie: Soziale Netzwerke, Blogs, Internetforen, Cloud-Dienste	126
7.2.4	Methoden zur endgültigen Datenvernichtung kennen, wie: Laufwerke/Datenträger zerstören, zB schreddern; Entmagnetisierung; Software zur Datenvernichtung verwenden.....	127
Wissens-Check		129
GLOSSAR		131
Zuletzt noch ein spannendes Rätsel		142
ANHANG		143
INDEX		145

Die Nummerierung der Inhaltsangabe nimmt Bezug auf den jeweiligen Punkt des Lernzielkatalogs (Version 3.0), den Sie unter <https://www.icdl.at/it-security> finden.