ICDL
The Digital Skills Standard

ICDL Workforce
IT-SICHERHEIT
Syllabus 2.0

Syllabus

icdl.org

Zweck

Dieses Dokument beschreibt den Lehrplan für das ICDL Modul IT-Sicherheit. Der Lehrplan beschreibt anhand der Lernziele die Kenntnisse und Fähigkeiten, die ein Kandidat für dieses Modul besitzen sollte. Der Lehrplan bildet auch die Grundlage für den theoretischen und praktischen Test zu diesem Modul.

Disclaimer

Obwohl bei der Erstellung dieser Publikation alle Sorgfalt aufgewendet wurde, übernimmt die ICDL Foundation als Herausgeber der englischen Originalversion keine Gewähr für die Vollständigkeit der darin enthaltenen Informationen. Weiterhin übernimmt die ICDL Foundation keine Verantwortung oder Haftung für etwaige Fehler, Auslassungen, Ungenauigkeiten, Verluste oder Schäden, die aufgrund von Informationen, Anweisungen oder Ratschlägen in dieser Veröffentlichung entstehen. Änderungen können von der ICDL Foundation nach eigenem Ermessen und jederzeit ohne vorherige Ankündigung vorgenommen werden.

IT-Sicherheit 2.0

Dieses Modul beinhaltet die wichtigsten Konzepte für den sicheren Umgang mit Informations- und Kommunikationstechnologie sowie die Kenntnisse und Fertigkeiten, die erforderlich sind, um eine sichere Netzwerkverbindung herzustellen, um sich im Internet gefahrlos bewegen zu können, und um sachgerecht mit Daten und Informationen umgehen zu können.

Ziele

Die Kandidatinnen und Kandidaten sollen:

- wichtige Konzepte zur Sicherung von Informationen und Daten kennen, um Identitätsdiebstahl, Betrug und Datendiebstahl vermeiden zu können,
- einen Computer, andere Geräte der IT-Technologie und Netzwerke vor Malware und unberechtigtem Zugriff schützen können,
- die Funktionsweise unterschiedlicher Netzwerktypen, Verbindungsarten und netzwerkspezifischer Programme und Techniken (z.B. Firewall) verstehen,
- sicher mit einem Browser im World Wide Web surfen und über das Internet kommunizieren können,
- verstehen, welche Sicherheitsprobleme bei der Kommunikation, z.B. mit E-Mail und Instant Messaging auftreten können,
- Daten sichern, rückspeichern und unwiederbringlich löschen können.

Kategorie	Wissensgebiet	Nr.	Lernziel
1 Sicherheits-konzepte	*1.1 Bedrohungen für Daten*	1.1.1	Daten und Informationen unterscheiden können.
		1.1.2	Den Begriff Cybercrime verstehen.
		1.1.3	Die Unterschiede zwischen Hacken, Cracken und ethischem Hacken verstehen.
		1.1.4	Bedrohungen von Daten durch höhere Gewalt, wie Feuer, Flut, Erdbeben und Krieg erkennen.
		1.1.5	Bedrohung von Daten durch Mitarbeiter, Service Provider und Dritte Personen erkennen.
	1.2 Den Wert von Informationen ein-schätzen können	1.2.1	Gefahren für persönliche Daten wie Identitätsdiebstahl und Betrug erkennen und abwehren können.
		1.2.2	Die Gefahren für sensible Geschäftsdaten wie Diebstahl und/oder Missbrauch von Kunden- und Finanzdaten verstehen.
		1.2.3	Maßnahmen gegen unautorisierten Zugriff auf Daten kennen: Passwort-schutz und Verschlüsselung.

Kategorie	Wissensgebiet	Nr.	Lernziel
		1.2.4	Die wesentlichen Eigenschaften von Informationssicherheit verstehen: Vertraulichkeit, Integrität und Verfügbarkeit.
		1.2.5	Die wichtigsten Datenschutz-bestimmungen, Anforderungen an die Datenaufbewahrung und -kontrolle im eigenen Land kennen.
		1.2.6	Die Bedeutung der Einführung und Einhaltung von Richtlinien in der Informations- und Kommunikations-technologie verstehen.
	1.3 persönliche Datensicherheit	1.3.1	Verstehen, was Social Engineering im Zusammenhang mit Datensicherheit ist: Betrug Datenbeschaffung, Zugang zu Systemen.
		1.3.2	Methoden des Social Engineering kennen: Telefongespräche, Phishing, shoulder surfing.
		1.3.3	Verstehen, was Identitätsdiebstahl ist und dessen Folgen kennen: persönlich, finanziell, geschäftlich, rechtlich.
		1.3.4	Methoden des Identitätsdiebstahls, wie Skimming, Pretexting und Information Diving kennen.
	1.4 Datensicherheit in Programmen	1.4.1	Verstehen, was es bedeutet, Makro-Sicherheitseinstellungen zu aktivieren oder deaktivieren.
		1.4.2	Einen Kennwortschutz für ein Dokument, ein Tabellenblatt oder eine gepackte Datei erstellen.
		1.4.3	Die Vorteile und Grenzen der Verschlüsselung von Daten verstehen.
2 Malware	*2.1 Definition und Funktionsweise*	2.1.1	Verstehen, was Malware ist.
		2.1.2	Wissen, wie Malware im System versteckt werden kann: Trojaner, RootKits oder Back Doors.
	2.2 Arten von Malware	2.2.1	Verschiedene Typen von Malware kennen und ihre Funktionsweise verstehen: Viren, Würmer
		2.2.2	Unterschiedliche Arten des Datendiebstahls und profitorientierter/erpresserischer Malware kennen und ihre Funktionsweise verstehen: Adware, Spyware, Botnets, keystroke logging, Dialer.

Kategorie	Wissensgebiet	Nr.	Lernziel
	2.3 Schutz vor Malware	2.3.1	Verstehen wie Anti-Virus Software arbeitet und die Grenzen des Schutzes kennen.
		2.3.2	Laufwerke, Ordner und Dateien mit Anti-Virus Software überprüfen können. Zeitgesteuerte Scans nutzen können. Die Möglichkeit der Quarantäne und deren Auswirkung auf infizierte Dateien kennen
		2.3.3	Verstehen, was Quarantäne bedeutet und was damit bewirkt wird.
		2.3.4	Die Wichtigkeit von regelmäßigen Updates der Anti-Virus Software kennen.
3 Netzwerk-sicherheit	*3.1 Netzwerke*	3.1.1	Verstehen, was ein Netzwerk ist und zwischen LAN, WAN und VPN unterscheiden können.
		3.1.2	Die Aufgaben des Netzwerk-administrators, wie Autorisierung, Authentifizierung Kontenvergabe für ein Netzwerkes verstehen.
		3.1.3	Funktionsweise und Leistungsgrenzen einer Firewall kennen.
	3.2 Netzwerk-verbindungen	3.2.1	Netzwerkverbindungen, wie Kabel- oder Funkverbindung kennen.
		3.2.2	Die möglichen Auswirkungen einer Netzwerkverbindung auf die Sicherheit verstehen: Malware, unberechtigter Datenzugriff, Gefährdung der Privatsphäre.
	3.3 Absicherung von drahtlosen Netzwerken	3.3.1	Die Bedeutung von Kennwörtern zum Schutz eines drahtlosen Netzwerkes kennen.
		3.3.2	Unterschiedliche Verschlüsselungen für Drahtlosnetzwerke kennen: WEP, WPA und MAC.
		3.3.3	Wissen und beachten, dass ein ungeschütztes Drahtlos-Netzwerk einem „Lauscher Zugang“ zu den Daten erlaubt.
		3.3.4	Sich mit einem geschützten/ ungeschützten Drahtlos-Netzwerk verbinden.

Kategorie	Wissensgebiet	Nr.	Lernziel
	3.4 Zugangskontrolle	3.4.1	Den Zweck eines Netzwerkkontos verstehen und dessen Sicherung durch Benutzername und Kennwort kennen.
		3.4.2	Wissen, wie ein gutes Passwort aufgebaut ist und wie man mit Passwörter umgehen sollte: nicht an Dritte weitergeben, regelmäßiges Ändern der Passwörter, ausreichende Passwortlänge und Zeichenfolge aus Buchstaben, Zahlen und Sonderzeichen.
		3.4.3	Biometrische Zugangskontrollen, wie Fingerabdruck und Iris-Scan kennen.
4 Sicherer Umgang mit Internetdiensten	*4.1 Surfen im Internet*	4.1.1	Wissen, dass für Onlinebanking und Online-Einkäufe nur sichere Internetseiten benutzt werden sollten.
		4.1.2	Eine sichere Internetseite identifizieren können: https, Schloss-Symbol.
		4.1.3	Sich der Gefahren von Pharming bewusst sein.
		4.1.4	Verstehen, was ein digitales Zertifikat ist. Die Gültigkeit eines digitalen Zertifikats überprüfen können.
		4.1.5	Wissen, was ein Einmal-Passwort ist.
		4.1.6	Die Einstellungen für das automatische Speichern und die automatische Vervollständigung eines Formulars auswählen, aktivieren und deaktivieren können.
		4.1.7	Verstehen, was ein Cookie ist.
		4.1.8	Die Browsereinstellungen zur Aktivierung/Deaktivierung von Cookies verwenden können.
		4.1.9	Persönliche Daten aus dem Browser löschen: Verlauf, Cache, Passwörter, Cookies, Daten zur automatischen Vervollständigung.
		4.1.10	Den Zweck und die Funktionsweise von Programmen zur Inhaltskontrolle von Webseiten kennen: Internet-Filter-Software, Software zur elterlichen Kontrolle.
	4.2 Social Networking (Soziale Netzwerke)	4.2.1	Verstehen, dass keine wichtigen Informationen auf Social Networking Seiten offengelegt werden sollten.

Kategorie	Wissensgebiet	Nr.	Lernziel
		4.2.2	Die Sicherheitseinstellungen für persönliche Daten auf Social Networking Seiten verstehen und anwenden können.
		4.2.3	Mögliche Gefahren von Social Networking Seiten verstehen: Cyber Bullying, Grooming, falsche Identitäten, betrügerische Nachrichten und Links.
5 Kommunikation	*5.1 E-Mail*	5.1.1	Den Zweck von Ver- und Entschlüsselung im E-Mail-Verkehr kennen.
		5.1.2	Den Begriff Digitale Signatur verstehen.
		5.1.3	Eine Digitale Signatur erstellen und einer E-Mail hinzufügen.
		5.1.4	Sich bewusst sein, dass man betrügerische und unerwünschte E-Mails erhalten kann.
		5.1.5	Verstehen, was Phishing ist und Phishing-Attacken an ihren typischen Eigenschaften erkennen: Verwendung von wirklichen Firmen- oder Personennamen, falsche Weblinks.
		5.1.6	Verstehen, dass beim Öffnen von Dateianhängen mit Makros oder ausführbaren Dateien der Computer durch Malware infiziert werden kann.
	5.2 Instant Messaging	5.2.1	Wissen, was Instant Messaging (IM) ist und die Anwendungsmöglichkeiten kennen.
		5.2.2	Die Gefährdung von Instant Messaging durch Malware, backdoor access, Datenzugriff verstehen.
		5.2.3	Methoden zur sicheren Nutzung von Instant Messaging (Verschlüsselung) kennen: Verschlüsselung, Nicht-Offenlegung wichtiger Daten, Beschränkung der gemeinsamen Dateinutzung.
6 Sicheres Daten-Management	*6.1 Datensicherung (Backup)*	6.1.1	Wissen, wie man Computer physisch durch Zugangskontrolle, Sicherheitskabel und geeignetem Standort schützen kann.
		6.1.2	Verstehen, dass Datensicherung notwendig ist, um der Gefahr des Datenverlustes vorzubeugen.
		6.1.3	Wichtige Bedingungen der Datensicherung kennen: Regelmäßige zeitgesteuerte Sicherung und sichere Lagerung.

Kategorie	Wissensgebiet	Nr.	Lernziel
		6.1.4	Ein Backup anlegen können.
		6.1.5	Daten zurücksichern und auf Richtigkeit überprüfen können.
	6.2 *Daten richtig löschen*	6.2.1	Gründe zur dauerhaften Löschung von Daten verstehen.
		6.2.2	Den Unterschied zwischen Löschen und der dauerhaften Datenvernichtung kennen.
		6.2.3	Methoden zur dauerhaften Vernichtung von Daten kennen: Shreddern, Zerstörung des Datenträgers, Entmagnetisierung (Degaussing), Verwendung von Programmen zur vollständigen Datenvernichtung.