

# Europäischer Computer Führerschein



## ECDL Modul IT-Sicherheit · Syllabus Version 1.0

DLGI mbH  
Am Bonner Bogen 6  
53227 Bonn  
Deutschland  
Tel.: 0228 - 688 448 10  
Fax.: 0228 - 688 448 99  
E-Mail: [info@dlgi.de](mailto:info@dlgi.de)  
URL: <http://www.ecdl.de>

Copyright © 2010 The ECDL Foundation Ltd.

Alle Rechte vorbehalten. Kein Teil dieser Publikation darf ohne Genehmigung der ECDL Foundation in irgendeiner Form reproduziert werden. Anfragen zur Genehmigung von Vervielfältigungen des Materials sind direkt an den Herausgeber zu stellen.

In Zweifelsfällen gilt die Version der ECDL Foundation, veröffentlicht auf [www.ecdl.org](http://www.ecdl.org). Dieser Syllabus darf nur in Zusammenhang mit der ECDL Initiative verwendet werden. Im Zusammenhang mit der ECDL Initiative ist dieser Syllabus zur Verwendung und Vervielfältigung freigegeben.

## **ECDL IT-Sicherheit** MODULZIELE

Das Modul ECDL / ICDL IT Sicherheit verlangt vom Prüfling ein grundlegendes Verständnis der wichtigsten Konzepte für den sicheren Umgang mit Informations- und Kommunikationstechnologie (ICT) im täglichen Arbeitsablauf. Er soll die relevanten Techniken und Programme kennen, um eine sichere Netzwerkverbindung herstellen und sich im Internet gefahrlos bewegen zu können sowie den Umgang mit Daten und Informationen angemessen bewältigen zu können.

### Der Kandidat soll

- Wichtige Konzepte zur Sicherung von Informationen und Daten kennen, um Identitätsdiebstahl, Betrug und Datendiebstahl zu vermeiden.
- Einen Computer, andere Geräte der IT-Technologie und Netzwerke vor Malware und unberechtigtem Zugriff schützen können.
- Die unterschiedlichen Netzwerktypen, Verbindungsarten und netzwerkspezifischen 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, wiederherstellen und unwiederbringlich löschen können.



Lehrstoff	Teilgebiet	Ref. Nr.	Lernziel
8.1 Sicherheitskonzepte	8.1.1 Bedrohungen für Ihre Daten	8.1.1.1	Daten und Informationen unterscheiden können.
		8.1.1.2	Den Begriff <i>Cybercrime</i> verstehen.
		8.1.1.3	Die Unterschiede zwischen <i>Hacken</i> , <i>Cracken</i> und <i>ethischem Hacken</i> verstehen.
		8.1.1.4	Bedrohungen von Daten durch höhere Gewalt, wie Feuer, Flut, Erdbeben und Krieg erkennen.
		8.1.1.5	Bedrohung von Daten durch Mitarbeiter, Service Provider und Dritte Personen erkennen.
	8.1.2 Den Wert von Informationen einschätzen können	8.1.2.1	Die Gefahren für persönliche Daten wie Identitätsdiebstahl und Betrug erkennen und abwehren können.
		8.1.2.2	Die Gefahren für sensible Geschäftsdaten wie Diebstahl und/oder Missbrauch von Kunden- und Finanzdaten verstehen.
		8.1.2.3	Maßnahmen gegen den unautorisierten Zugriff auf Daten kennen: Verschlüsselung und Passwortschutz.
		8.1.2.4	Die wesentlichen Eigenschaften von Informationssicherheit verstehen: Vertraulichkeit, Integrität und Verfügbarkeit.
		8.1.2.5	Die wichtigsten Datenschutzbestimmungen, Anforderungen an die Datenaufbewahrung und Kontrolle im eigenen Land kennen.
		8.1.2.6	Die Bedeutung der Einführung und Einhaltung von Richtlinien in der ICT verstehen.
	8.1.3 persönliche Datensicherheit	8.1.3.1	Den Begriff <i>Social Engineering</i> im Zusammenhang mit Datensicherheit verstehen: Datenbeschaffung, Betrug, Zugang zu Computersystemen.

Lehrstoff	Teilgebiet	Ref. Nr.	Lernziel
		8.1.3.2	Methoden des <i>Social Engineering</i> kennen: Telefonanrufe, <i>Phishing</i> , <i>Shoulder Surfing</i> .
		8.1.3.3	Den Begriff Identitätsdiebstahl und dessen Folgen verstehen: personenbezogen, finanziell, geschäftlich, rechtlich.
		8.1.3.4	Methoden des Identitätsdiebstahls, wie <i>Skimming</i> , <i>Pretexting</i> und <i>Information Diving</i> kennen.
	8.1.4 Datensicherheit in Programmen	8.1.4.1	Verstehen, was es bedeutet, Macro-Sicherheitseinstellungen zu aktivieren oder deaktivieren.
		8.1.4.2	Einen Kennwortschutz für ein Dokument, ein Tabellenblatt oder eine komprimierte Datei erstellen.
		8.1.4.3	Die Vorteile und Grenzen der Verschlüsselung von Daten verstehen.
8.2 Malware	8.2.1 Definition und Funktionsweise	8.2.1.1	Den Begriff Malware verstehen.
		8.2.1.2	Sich der verschiedenen Möglichkeiten bewusst sein, Malware im System zu verstecken: Trojaner, <i>RootKits</i> oder <i>Back Doors</i> .
	8.2.2 Arten von Malware	8.2.2.1	Verschiedene Typen von Malware erkennen und ihre Funktionsweise verstehen: Viren, Würmer
		8.2.2.2	Unterschiedliche Arten des Datendiebstahls und profitorientierter/ erpresserischer Malware erkennen und ihre Funktionsweise verstehen: <i>Adware</i> , <i>Spyware</i> , <i>Botnets</i> , <i>Keystroke Logging</i> , <i>Dialer</i> .
	8.2.3 Schutz vor Malware	8.2.3.1	Verstehen wie Anti-Virus Software arbeitet und die Grenzen des Schutzes kennen.
		8.2.3.2	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

Lehrstoff	Teilgebiet	Ref. Nr.	Lernziel
		8.2.3.3	Den Begriff Quarantäne verstehen und verstehen, was damit bewirkt wird.
		8.2.3.4	Die Wichtigkeit von regelmäßigen Updates der Anti-Virus Software kennen.
8.3 Netzwerksicherheit	8.3.1 Netzwerke	8.3.1.1	Den Begriff Netzwerk verstehen und zwischen LAN, WAN und VPN unterscheiden können.
		8.3.1.2	Die Aufgaben des Netzwerkadministrators, wie Autorisierung, Authentifizierung, Kontenvergabe innerhalb eines Netzwerkes verstehen.
		8.3.1.3	Funktionsweise und Leistungsgrenzen einer Firewall kennen.
	8.3.2 Netzwerkverbindungen	8.3.2.1	Unterschiedliche Netzwerkverbindungen kennen: z.B. Kabel- oder Funkverbindung.
		8.3.2.2	Die möglichen Auswirkungen einer Netzwerkverbindung auf die Sicherheit verstehen: <i>Malware</i> , unberechtigter Datenzugriff, Gefährdung der Privatsphäre.
	8.3.3 Absicherung von drahtlosen Netzwerken	8.3.3.1	Die Bedeutung von Kennwörtern zum Schutz eines drahtlosen Netzwerkes erkennen.
		8.3.3.2	Unterschiedliche Verschlüsselungen für Drahtlosnetzwerke kennen: WEP, WPA und MAC.
		8.3.3.3	Sich bewusst sein, dass ein ungeschütztes Drahtlosnetzwerk einem <i>Lauscher</i> den Zugang zu Ihren Daten erlaubt.
		8.3.3.4	Sich rechtmäßig mit einem geschützten/ungeschützten Drahtlos-Netzwerk verbinden.
	8.3.4 Zugangskontrolle	8.3.4.1	Den Zweck eines Netzwerkkontos verstehen und dessen Sicherung durch Benutzername und Kennwort kennen.

Lehrstoff	Teilgebiet	Ref. Nr.	Lernziel
		8.3.4.2	Wissen, wie ein gutes Passwort aufgebaut ist und wie man mit Passwörtern umgehen sollte: keine Weitergabe an Dritte, regelmäßiges Ändern der Passwörter, entsprechende Passwortlänge und Zeichenfolge aus Buchstaben, Zahlen und Sonderzeichen.
		8.3.4.3	Biometrische Zugangskontrollen, wie Fingerabdruck und Iris-Scan kennen.
8.4 Sicherer Umgang mit Internetdiensten	8.4.1 Surfen im Internet	8.4.1.1	Wissen, dass für Onlinebanking und Online-Einkäufe nur sichere Internetseiten benutzt werden sollten.
		8.4.1.2	Eine sichere Internetseite erkennen können: https, Schloss-Symbol.
		8.4.1.3	Sich der Gefahren von <i>Pharming</i> bewusst sein.
		8.4.1.4	Den Begriff <i>Digitales Zertifikat</i> verstehen und dessen Gültigkeit überprüfen können.
		8.4.1.5	Den Begriff Einmal-Passwort verstehen.
		8.4.1.6	Die Einstellungen für das automatische Speichern und die automatische Vervollständigung eines Formular auswählen, aktivieren und deaktivieren können.
		8.4.1.7	Den Begriff <i>Cookie</i> verstehen.
		8.4.1.8	Die Browsereinstellungen zur Aktivierung/Deaktivierung von Cookies verwenden können.
		8.4.1.9	Persönliche Daten aus dem Browser löschen: Verlauf, <i>Cache</i> , Passwörter, <i>Cookies</i> , Daten zur automatischen Vervollständigung.
		8.4.1.10	Den Zweck und die Funktionen von Programmen zur Inhaltskontrolle von Webseiten kennen: Internet-Filter-Software, Software zur elterlichen Kontrolle.

Lehrstoff	Teilgebiet	Ref. Nr.	Lernziel
	8.4.2 Social Networking (Soziale Netzwerke)	8.4.2.1	Verstehen, dass keine wichtigen Informationen auf Social Networking Seiten offengelegt werden sollten.
		8.4.2.2	Die Sicherheitseinstellungen für persönliche Daten auf <i>Social Networking</i> Seiten verstehen und anwenden können.
		8.4.2.3	Mögliche Gefahren von <i>Social Networking</i> Seiten verstehen: <i>Cyber Bullying, Grooming</i> , falsche Identitäten, betrügerische Nachrichten und Links.
8.5 Kommunikation	8.5.1 E-Mail	8.5.1.1	Den Zweck von Ver- und Entschlüsselung im E-Mail-Verkehr kennen.
		8.5.1.2	Den Begriff Digitale Signatur verstehen.
		8.5.1.3	Eine Digitale Signatur erstellen und einer E-Mail hinzufügen.
		8.5.1.4	Sich bewusst sein, dass man betrügerische und unerwünschte E-Mails erhalten kann.
		8.5.1.5	Den Begriff <i>Phishing</i> verstehen und <i>Phishing</i> -Attacken an ihren typischen Eigenschaften erkennen: Verwendung von wirklichen Firmen- oder Personennamen, falsche Weblinks.
		8.5.1.6	Sich der Gefahr bewusst sein, dass beim Öffnen von Dateianhängen mit Makros oder ausführbaren Dateien der Computer durch <i>Malware</i> infiziert werden kann.
	8.5.2 Instant Messaging	8.5.2.1	Den Begriff Instant Messaging (IM) und die Anwendungsmöglichkeiten kennen.
		8.5.2.2	Die Gefährdung von Instant Messaging durch <i>Malware, Backdoor Access</i> , Datenzugriff verstehen.



Lehrstoff	Teilgebiet	Ref. Nr.	Lernziel
		8.5.2.3	Methoden zur sicheren Nutzung von <i>Instant Messaging</i> (Verschlüsselung) kennen: Verschlüsselung, Nicht-Offenlegung wichtiger Daten, Beschränkung der gemeinsamen Dateinutzung.
8.6 Sicheres Daten-Management	8.6.1 Datensicherung	8.6.1.1	Wissen, wie man Computer physisch durch Zugangskontrolle, Sicherheitskabel und einen geeigneten Standort schützen kann.
		8.6.1.2	Verstehen, dass Datensicherung (Backup) notwendig ist, um der Gefahr des Datenverlustes vorzubeugen.
		8.6.1.3	Wichtige Eigenschaften einer Datensicherung kennen: Regelmäßige, zeitgesteuerte Sicherung, sichere Aufbewahrung.
		8.6.1.4	Ein <i>Backup</i> erstellen können.
		8.6.1.5	Daten wiederherstellen und auf Richtigkeit überprüfen können.
	8.6.2 Daten richtig löschen	8.6.2.1	Den Zweck und die Gründe zur endgültigen Datenvernichtung verstehen.
		8.6.2.2	Den Unterschied zwischen Löschen und endgültiger Datenvernichtung kennen.
		8.6.2.3	Methoden zur endgültigen Vernichtung von Daten kennen: <i>Shreddern</i> , Vernichtung des Datenträgers, Entmagnetisierung ( <i>Degaussing</i> ), Verwendung von Programmen zur vollständigen Datenvernichtung..