



OCG
IT-Security

CERTIFICATION FOR USERS



OCG IT-Security

OCG IT-Security

Lernzielkatalog **2.0**
Syllabus Version

OCG

Österreichische Computer Gesellschaft
Wollzeile 1-3, 1010 Wien
Tel: + 43 1 512 02 35-0
Fax: + 43 1 512 02 35-9
E-Mail: ocg@ocg.at
Web: www.ocg.at

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. In Zweifelsfällen gilt die Version der OCG, veröffentlicht auf www.ocg.at

Urheberrecht: © Österreichische Computer Gesellschaft (OCG) 2011
Alle Rechte vorbehalten.

Dieser Syllabus darf nur in Zusammenhang mit dem Zertifikatsprogramm der OCG verwendet werden.

Geschlechtsbezogene Aussagen in diesem Syllabus sind auf Grund der Gleichstellung für beiderlei Geschlechter aufzufassen bzw. auszulegen.

Der Syllabus wurde in Zusammenarbeit mit dem ersten Kompetenzzentrum für organisatorische und technische Aspekte von IT-Security, Secure Business Austria (SBA), sowie in Abstimmung mit dem Zentrum für sichere Informationstechnologie, A-SIT, erstellt.

OCG IT-Security

OCG IT-Security ermöglicht eine praxisrelevante Steigerung des Wissens um die wichtigsten Aspekte der IT-Sicherheit im Umgang mit vernetzten Computersystemen.

- 1 Informationssicherheit
- 2 Verschiedene Bedrohungen kennen
- 3 Wichtige Begriffe kennen
- 4 Social Engineering
- 5 IT-Sicherheit in der Praxis anwenden
- 6 Mobile Sicherheit
- 7 Sicherheit von Informationen in Onlinediensten
- 8 Physische Sicherheit und Datensicherheit

IT-Security Syllabus Version 2.0

ZIELE

Zielgruppe für das OCG Zertifikat IT-Security sind Computeranwender, die sich mit den wichtigsten Sicherheitsaspekten im Umgang mit Informations- und Kommunikationstechnologien vertraut machen wollen.

Ziel des Zertifikats ist es, das Vertrauen der Benutzer in IT und Internetanwendungen zu erhöhen und gleichzeitig das Wissen um die Gefahren und deren Vermeidung bei der täglichen Arbeit zu verbessern.

Voraussetzungen sind ein allgemeines Grundwissen über Personal Computer und Betriebssysteme, Basiswissen über gängige Office-Anwendungen sowie über die Nutzung von Internet und E-Mail-Diensten.

Die Inhalte von OCG IT-Security sind speziell an den Endbenutzer angepasst und ermöglichen eine praxisrelevante Steigerung des Wissens um die wichtigsten Aspekte der IT-Sicherheit im Umgang mit vernetzten Computersystemen. Dabei werden technische Hintergründe nur soweit behandelt, wie sie für das Grundverständnis der Probleme und Lösungsmöglichkeiten unerlässlich sind.

Durch die dynamischen Eigenschaften des Internets werden die aktuellsten Entwicklungen im Bereich der Computersicherheit, zum Beispiel die stark steigende Verbreitung von Smartphones, die erfolgreiche Vermarktung von Cloud Computing und der große Erfolg von sozialen Netzwerken wie Facebook, thematisiert.

Kategorie	Wissensgebiet	Ref.	Fertigkeit
1 Informationssicherheit	1.1 Wert von Informationen	1.1.1	Den Wert von Daten und Informationen abschätzen können
		1.1.2	Informationen klassifizieren
		1.1.3	Grundsätzlichen Umgang mit Risiken verstehen
	1.2 Anforderungen an die Informationssicherheit	1.2.1	Vertraulichkeit, Integrität und Verfügbarkeit verstehen
		1.2.2	Die Anforderung nach Nicht-Abstreitbarkeit, Nachvollziehbarkeit, Authentizität verstehen
2 Verschiedene Bedrohungen	2.1 Umwelt	2.1.1	Bedrohung von Daten durch höhere Gewalt kennen
		2.1.2	Bedrohungen der Infrastruktur kennen
	2.2 Personen	2.2.1	Bedrohung von Daten durch interne Personen verstehen

Kategorie	Wissensgebiet	Ref.	Fertigkeit
		2.2.2	Bedrohung von Daten durch Mittler verstehen wie zB Wartungspersonal, Zeitarbeiter, Praktikanten
		2.2.3	Bedrohung von Daten durch externe Personen verstehen
	2.3 Kriminalität im Internet	2.3.1	Die Bedeutung des Begriffes „Cybercrime“ kennen
		2.3.2	Wissen wie Kriminelle im Internet Geld verdienen
3 Wichtige Begriffe	3.1 Grundsätzliches Verständnis	3.1.1	Wichtige allgemeine Begriffe der IT-Sicherheit kennen und verstehen
		3.1.2	Phishing, Malicious Code: Begriffe aus der Welt der Hacker und Script-Kiddies kennen und verstehen
4 Social Engineering	4.1 Social Engineering	4.1.1	Social Engineering Angriffe verstehen und vermeiden
		4.1.2	Verschiedene Formen von Social Engineering kennen
		4.1.3	Dumpster Diving und Shoulder Surfing erkennen und vermeiden
5 IT-Sicherheit in der Praxis	5.1 Sicherheit im Betriebssystem	5.1.1	Merkmale eines guten Passworts kennen
		5.1.2	Biometrische Zugangssysteme verstehen
		5.1.3	Das Ereignisprotokoll überprüfen können
		5.1.4	Dateien und Ordner vollständig löschen können
		5.1.5	Bedeutung unterschiedlicher Benutzerrechte verstehen
	5.2 Eine Personal Firewall verstehen und verwenden	5.2.1	Möglichkeiten und Einschränkungen von Personal Firewalls kennen
		5.2.2	Meldungen und Nachfragen von Personal Firewalls verstehen
	5.3 Einen Virens scanner auswählen	5.3.1	Grundsätzliche Funktionsweise von Virenscannern verstehen
		5.3.2	Kriterien für die Auswahl von Virenscannern kennen
		5.3.3	Grenzen der Virens scanner kennen
	5.4 Sicherheit in Anwendungen	5.4.1	Die Gefahren von aktiven Inhalten verstehen und vermeiden

Kategorie	Wissensgebiet	Ref.	Fertigkeit
		5.4.2	Passwortschutz in Office-Produkten einsetzen und verstehen
		5.4.3	Unerwünschte Spuren in Office- und Adobe Acrobat-Dokumenten vermeiden
		5.4.4	Dokumenten-Signatur verstehen und anwenden
	5.5 E-Mail-Sicherheit	5.5.1	Unterschied zwischen Signieren und Verschlüsseln verstehen
		5.5.2	Eine E-Mail ver- bzw. entschlüsseln
		5.5.3	Eine E-Mail signieren
		5.5.4	E-Mail-Sicherheit konfigurieren
		5.5.5	Phishing-Angriffe erkennen
	5.6 Web-Sicherheit	5.6.1	Internet-Zonen einrichten
		5.6.2	Cross Site Scripting-Angriffe erkennen
		5.6.3	Zertifikate von Webseiten prüfen
		5.6.4	Kreditkarten im Internet sicher benutzen
		5.6.5	Die Gefahren von Online-Versteigerungen und Online-Shopping richtig einschätzen und vermeiden
		5.6.6	Eine URL (Unified Resource Locator) lesen und interpretieren können
6 Mobile Sicherheit	6.1 Laptop	6.1.1	Daten auf Laptops verschlüsseln und absichern
	6.2 PDA und Smartphone	6.2.1	Wissen wie Smartphones und PDAs abgesichert und verschlüsselt werden
		6.2.2	Wissen um die Gefahren die von Applikationen auf Smartphones ausgehen
	6.3 WLAN und WIFI Sicherheit	6.3.1	Unsichere WLANs (Wireless LAN) verstehen und erkennen
		6.3.2	Schwächen von WEP (Wireless Encryption Protocol), Mac (Media Access Control)-Filter und WPA (Wi-Fi protected access) verstehen
		6.3.3	Sicheres WLAN mit WPA konfigurieren
	6.4 VPNs	6.4.1	VPNs (Virtuelle Private Netzwerke) verstehen
		6.4.2	VPN-Verbindungen überprüfen
	6.5 Firewalls	6.5.1	Funktion einer Firmen-Firewall verstehen

Kategorie	Wissensgebiet	Ref.	Fertigkeit	
		6.5.2	Ein Heimnetz sicher mit dem Internet verbinden	
7 Sicherheit von Informationen in Onlinediensten	7.1 Soziale Netzwerke	7.1.1	Mögliche Gefahren in sozialen Netzen kennen	
		7.1.2	Wissen um die Wichtigkeit des Schutzes der Privatsphäre im Internet	
		7.1.3	Technische Schutzmaßnahmen in sozialen Netzwerken kennen und anwenden	
		7.1.4	Mögliche Gefahren bei weiteren Onlineservices, wie Skype und anderen Chatprogrammen kennen	
	7.2 Cloud	7.2.1	Gefahren, Möglichkeiten und Grenzen von ComputingCloud Computing und Online Speicherdiensten kennen	
		7.2.2	Online Speicherdienste und Cloud Computing richtig nutzen	
8 Physische Sicherheit und Datensicherheit	8.1 Physische Schutzmaßnahmen	8.1.1	PC-Komponenten physisch sichern	
		8.1.2	Physische Sicherheitsmaßnahmen bei mobilen Geräten verwenden	
		8.1.3	Physische Schutzmaßnahmen in Gebäuden erkennen und überprüfen	
		8.2 Datensicherheit	8.2.1	Möglichkeiten der Datensicherung kennen und unterscheiden können
	8.2.2		Eine Datensicherungsstrategie verstehen und planen können	
	8.2.3		Wissen wie man sich im Falle eines Datenverlustes richtig verhält	
	8.2.4		Backup wichtiger Daten und Systeminformationen anlegen	
	8.2.5		Durchführung der Backup-Jobs kontrollieren und Backup auf Korrektheit prüfen	
	8.2.6		Magnetische Medien (Datenträger) richtig entsorgen	
	8.2.7		Optische Medien sicher entsorgen	

Ihr autorisiertes Test Center

OCG IT-Security

OCG



OESTERREICHISCHE
COMPUTER GESELLSCHAFT[®]
AUSTRIAN
COMPUTER SOCIETY

Österreichische Computer Gesellschaft
Wollzeile 1-3, 1010 Wien, Tel + 43 1 512 02 35-0
ocg@ocg.at, www.ocg.at