ECDL Foundation

AICA
Associazione Italiana per l'Informatica ed il Calcolo Automatico

EUROPEAN COMPUTER DRIVING LICENCE

IT Security

Syllabus

Scopo

Questo documento presenta il syllabus di *ECDL Standard – IT Security*. Il syllabus descrive, attraverso i risultati del processo di apprendimento, la conoscenza e le capacità di un candidato. Il syllabus fornisce inoltre le basi per il test teorico e pratico relativo a questo modulo.

Nota del traduttore

La versione ufficiale in lingua inglese del Syllabus ECDL Versione 1.0 è quella pubblicata sul sito web della Fondazione ECDL che si trova all'indirizzo **www.ecdl.org**. La presente versione italiana è stata tradotta a cura di AICA e rilasciata nel mese di maggio 2013.

Tanto la natura "definitoria" del testo, quanto la sua forma schematica costituiscono ostacoli di fronte ai quali è necessario trovare qualche compromesso; pur cercando di rendere al meglio in lingua italiana i concetti espressi nell'originale inglese, in alcuni casi sono evidenti i limiti derivanti dall'uso di un solo vocabolo per tradurre una parola inglese. Tale limite è particolarmente riduttivo per i verbi che dovrebbero identificare con maggiore esattezza i requisiti di conoscenza o competenza: moltissime voci contengono verbi come *understand*, *know*, *know about*, che sono stati solitamente tradotti con "comprendere", "conoscere", "sapere", ma che potrebbero valere anche per "capire", "intendere", "definire", "riconoscere", "essere a conoscenza"...
Per alcuni vocaboli tecnici è inoltre invalso nella lingua l'uso del termine inglese (es. *hardware*, *software*), e in molti casi – pur cercando di non assecondare oltre misura questa tendenza – si è ritenuto più efficace attenersi al vocabolo originale o riportarlo tra parentesi per maggior chiarezza.
Si invitano i lettori che abbiano particolari esigenze di analisi approfondita dei contenuti a fare riferimento anche alla versione inglese di cui si è detto sopra.

Limitazione di responsabilità

Benché la Fondazione ECDL abbia messo ogni cura nella preparazione di questa pubblicazione, la Fondazione ECDL non fornisce alcuna garanzia come editore riguardo la completezza delle informazioni contenute, né potrà essere considerata responsabile per eventuali errori, omissioni, inaccuratezze, perdite o danni eventualmente arrecati a causa di tali informazioni, ovvero istruzioni ovvero consigli contenuti nella pubblicazione. Le informazioni contenute in questa pubblicazione non possono essere riprodotte né nella loro interezza né parzialmente senza il permesso e il riconoscimento ufficiale da parte della Fondazione ECDL. La Fondazione ECDL può effettuare modifiche a propria discrezione e in qualsiasi momento senza darne notifica.

[1] Tutti i riferimenti alla Fondazione ECDL riguardano la European Computer Driving Licence Foundation Ltd.

IT Security

Il presente modulo *ECDL Standard – IT Security* definisce i concetti e le competenze fondamentali per comprendere l'uso sicuro dell'ICT nelle attività quotidiane e per utilizzare tecniche e applicazioni rilevanti che consentono di gestire una connessione di rete sicura, usare Internet in modo sicuro e senza rischi e gestire in modo adeguato dati e informazioni.

Scopi del modulo

Chi supera la prova d'esame per questo modulo è in grado di:

- Comprendere i concetti fondamentali relativi all'importanza di rendere sicure informazioni e dati, di assicurare protezione fisica e privacy, e di difendersi dal furto di identità.
- Proteggere un computer, un dispositivo o una rete da malware e da accessi non autorizzati.
- Comprendere i tipi di reti, i tipi di connessioni e le problematiche specifiche alle reti, firewall inclusi.
- Navigare nel World Wide Web e comunicare in modo sicuro su Internet.
- Comprendere i problemi di sicurezza associati alle comunicazioni, inclusa la posta elettronica e la messaggistica istantanea.
- Effettuare copie di sicurezza e ripristinare i dati in modo corretto e sicuro, ed eliminare dati e dispositivi in modo sicuro.

SEZIONE	TEMA	RIF.	Argomento
1 Concetti di sicurezza	*1.1 Minacce ai dati*	1.1.1	Distinguere tra dati e informazioni.
		1.1.2	Comprendere il termine crimine informatico.
		1.1.3	Comprendere la differenza tra hacking, cracking e hacking etico.
		1.1.4	Riconoscere le minacce ai dati provocate da forza maggiore, quali fuoco, inondazione, guerra, terremoto.
		1.1.5	Riconoscere le minacce ai dati provocate da impiegati, fornitori di servizi e persone esterne.
	1.2. Valore delle informazioni	1.2.1	Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi.
		1.2.2	Comprendere i motivi per proteggere informazioni commercialmente sensibili, quali prevenzione di furti, di uso improprio dei dati dei clienti o di informazioni finanziarie.
		1.2.3	Identificare le misure per prevenire accessi non autorizzati ai dati, quali cifratura, password.
		1.2.4	Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali confidenzialità, integrità, disponibilità.
		1.2.5	Identificare i requisiti principali per la protezione, conservazione e controllo di dati/privacy che si applicano in Italia.
		1.2.6	Comprendere l'importanza di creare e attenersi a linee guida e politiche per l'uso dell'ICT.
	1.3 Sicurezza personale	1.3.1	Comprendere il termine "ingegneria sociale" e le sue implicazioni, quali raccolta di informazioni, frodi e accesso a sistemi informatici.

SEZIONE	TEMA	RIF.	Argomento
		1.3.2	Identificare i metodi applicati dall'ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing al fine di carpire informazioni personali.
		1.3.3	Comprendere il termine furto di identità e le sue implicazioni personali, finanziarie, lavorative, legali.
		1.3.4	Identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati, fingendosi qualcun altro o mediante skimming.
	1.4 Sicurezza dei file	1.4.1	Comprendere l'effetto di attivare/disattivare le impostazioni di sicurezza delle macro.
		1.4.2	Impostare una password per file quali documenti, file compressi, fogli di calcolo.
		1.4.3	Comprendere i vantaggi e i limiti della cifratura.
2 Malware	*2.1 Definizione e funzione*	2.1.1	Comprendere il termine malware.
		2.1.2	Riconoscere diversi modi con cui il malware si può nascondere, quali trojan, rootkit e backdoor.
	2.2 Tipi	2.2.1	Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio virus e worm.
		2.2.2	Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio adware, spyware, botnet, keylogger e dialer.
	2.3 Protezione	2.3.1	Comprendere come funziona il software anti-virus e quali limitazioni presenta.
		2.3.2	Eseguire scansioni di specifiche unità, cartelle, file usando un software anti-virus. Pianificare scansioni usando un software anti-virus.
		2.3.3	Comprendere il termine quarantena e l'operazione di mettere in quarantena file infetti/sospetti.
		2.3.4	Comprendere l'importanza di scaricare e installare aggiornamenti di software, file di definizione di anti-virus.
3 Sicurezza in rete	*3.1 Reti*	3.1.1	Comprendere il termine rete e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WAN (rete geografica), VPN (rete privata virtuale).
		3.1.2	Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete.
		3.1.3	Comprendere la funzione e i limiti di un firewall.
	3.2 Connessioni di rete	3.2.1	Riconoscere le possibilità di connessione ad una rete mediante cavo o wireless.
		3.2.2	Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, mantenimento della privacy.
	3.3 Sicurezza su reti wireless	3.3.1	Riconoscere l'importanza di richiedere una password per proteggere gli accessi a reti wireless.

SEZIONE	TEMA	RIF.	Argomento
		3.3.2	Riconoscere diversi tipi di sicurezza per reti wireless, quali WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), MAC (Media Access Control).
		3.3.3	Essere consapevoli che usando una rete wireless non protetta si rischia che i propri dati vengano intercettati da “spie digitali”.
		3.3.4	Connettersi ad una rete wireless protetta/non protetta.
	3.4 Controllo di accesso	3.4.1	Comprendere lo scopo di un account di rete e come accedere alla rete usando un nome utente e una password.
		3.4.2	Riconoscere buone politiche per la password, quali evitare di condividere le password, modificarle con regolarità, sceglierle di lunghezza adeguata e contenenti un numero accettabile di lettere, numeri e caratteri speciali.
		3.4.3	Identificare le comuni tecniche di sicurezza biometriche usate per il controllo degli accessi, quali impronte digitali, scansione dell’occhio.
4 Uso sicuro del web	*4.1 Navigazione in rete*	4.1.1	Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) dovrebbero essere eseguite solo su pagine web sicure.
		4.1.2	Identificare un sito web sicuro, ad esempio associato ad https, simbolo del lucchetto.
		4.1.3	Essere consapevoli del pharming.
		4.1.4	Comprendere il termine “certificato digitale”. Convalidare un certificato digitale.
		4.1.5	Comprendere il termine “one-time password”.
		4.1.6	Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo.
		4.1.7	Comprendere il termine “cookie”.
		4.1.8	Selezionare impostazioni adeguate per consentire, bloccare i cookie.
		4.1.9	Eliminare dati privati da un browser, quali cronologia di navigazione, file temporanei di internet, password, cookie, dati per il completamento automatico.
		4.1.10	Comprendere lo scopo, la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori.
	4.2 Reti sociali	4.2.1	Comprendere l’importanza di non divulgare informazioni riservate su siti di reti sociali.
		4.2.2	Essere consapevoli della necessità di applicare impostazioni adeguate per la privacy del proprio account su una rete sociale.

SEZIONE	TEMA	RIF.	Argomento
		4.2.3	Comprendere i rischi potenziali durante l'uso di siti di reti sociali, quali cyberbullismo, adescamento, informazioni fuorvianti/pericolose, false identità, link o messaggi fraudolenti.
5 Comunicazioni	*5.1 Posta elettronica*	5.1.1	Comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica.
		5.1.2	Comprendere il termine firma digitale.
		5.1.3	Creare e aggiungere una firma digitale.
		5.1.4	Essere consapevoli della possibilità di ricevere messaggi fraudolenti e non richiesti.
		5.1.5	Comprendere il termine phishing. Identificare le più comuni caratteristiche del phishing, quali uso del nome di aziende e persone autentiche, collegamenti a falsi siti web.
		5.1.6	Essere consapevoli del rischio di infettare il computer con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile.
	5.2 Messaggistica istantanea	5.2.1	Comprendere il termine messaggistica istantanea (IM) e i suoi usi.
		5.2.2	Comprendere le vulnerabilità di sicurezza della messaggistica istantanea, quali malware, accesso da backdoor, accesso a file.
		5.2.3	Riconoscere metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea, quali cifratura, non divulgazione di informazioni importanti, limitazione di condivisione di file.
6 Gestione sicura dei dati	*6.1 Messa in sicurezza e salvataggio di dati*	6.1.1	Riconoscere modi per assicurare la sicurezza fisica di dispositivi, quali registrare la collocazione e i dettagli degli apparati, usare cavi di sicurezza, controllare gli accessi.
		6.1.2	Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati, di informazioni finanziarie, di segnalibri/cronologia web.
		6.1.3	Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione della memoria di massa.
		6.1.4	Effettuare la copia di sicurezza di dati.
		6.1.5	Ripristinare e validare i dati sottoposti a copia di sicurezza.
	6.2 Distruzione sicura	6.2.1	Comprendere il motivo per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi.
		6.2.2	Distinguere tra cancellare i dati e distruggerli in modo permanente.

SEZIONE	TEMA	RIF.	Argomento
		6.2.3	Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di utilità per la cancellazione definitiva dei dati.

