ECDL Foundation

ECDL / ICDL Сигурност в Информационните технологии

Учебна програма

Цел

Този документ съдържа подробна информация относно учебната програма за модул *ECDL / ICDL Сигурност в информационните технологии.* Учебната програма очертава знанията и уменията, които кандидатът за *ECDL / ICDL Сигурност в информационните технологии* трябва да притежава. Освен това учебната програма предоставя необходимата основа за теоретически и практически базирания тест в този модул.

Забележка

Въпреки че Фондация ECDL е взела всички мерки при подготвянето на настоящата публикация, тя не дава гаранция в качеството си на издател за пълнотата на информацията. Тя няма да бъде отговорна за каквито и да е грешки, пропуски, неточности, загуби или вреди, причинени от непълна информация, инструкции или съвети, съдържащи се в настоящата публикация. Фондация ECDL може да направи промени по своя преценка по всяко време, без предупреждение.

ECDL / ICDL Сигурност в Информационните Технологии

Този модул представя най-важните понятия и умения, свързани със сигурността при употреба на информационните и комуникационни технологии в ежедневието. Той дава и съществена информация при използване на съответните техники и приложения за поддръжка на сигурна мрежова връзка, както и безопасност при използване на интернет и управление на данни.

Цели на модула

Изисквания към изпитвания:

- Разбиране на основните понятия относно сигурност на информация и данни, физическа сигурност, поверителност и кражба на самоличност
- Защита на компютър, устройство или мрежа от зловреден софтуер (malware) и неоторизиран достъп
- Разбиране на типовете мрежи, връзки и специфични теми като защитна стена на компютъра (firewall)
- Безопасна работа в уеб пространството и комуникация в интернет
- Безопасна комуникация по електронна поща (e-mail) и програми за мигновени съобщения (instant messaging)
- Създаване и възстановяване на резервно копие на данни (back up) правилно и безопасно, както и сигурно премахване на данни и устройства

КАТЕГОРИЯ	УМЕНИЯ	РЕФ.	ЗАДАЧИ
1 Понятия, свързани със сигурността	1.1 Заплахи за данни	1.1.1	Различия между данни и информация.
		1.1.2	Запознаване с термина кибер престъпление (cybercrime).
		1.1.3	Разбиране на различията между хакване, кракване и етично хакване (hacking, cracking and ethical hacking).
		1.1.4	Форсмажорни заплахи за данни от: пожар, наводнение, война, земетресение.
		1.1.5	Заплахи за данни от: служители, доставчици на услуги и външни индивиди.
	1.2 Стойност на информацията	1.2.1	Разбиране на причините за предпазване на лична информация като: избягване на кражба на самоличност и измама.
		1.2.2	Разбиране на причините за предпазване на чувствителна търговска информация като: предотвратяване на кражба или злоупотреба с информация на клиенти и финансова информация.
		1.2.3	Мерки за предотвратяване на непозволен достъп до данни като: криптиране (encryption), пароли (passwords).
		1.2.4	Разбиране на основни характеристики на безопасността на информацията като: поверителност, почтеност, достъпност.

		1.2.5	Определяне на основните изисквания за предпазване, задържане и контрол на данни/поверителност във вашата държава.
		1.2.6	Разбиране на важността от създаване на насоки и спазване на политики при употреба на информационни и комуникационни технологии (ICT).
	1.3 Лична сигурност	1.3.1	Запознаване с термина социално инженерство (social engineering) и последиците от него като: събиране на информация, измама, достъп до компютърни системи.
		1.3.2	Идентифициране на методи за социално инженерство като телефонни обаждания, фишинг (phishing), сърфиране „през рамо“ (shoulder surfing).
		1.3.3	Разбиране на термина кражба на самоличност и последиците от него: лични, финансови, правни, свързани с бизнеса.
		1.3.4	Идентифициране на методи за кражба на самоличност: събиране на информация от устройства, които не се употребяват вече (information diving), измама чрез скимиране (skimming), измама чрез фалшиви мотиви (pretexting).
	1.4 Сигурност на фйлове	1.4.1	Разбиране на ефекта от включване/изключване на макро настройки за сигурност.
		1.4.2	Задаване на пароли за файлове като: документи, компресирани файлове, таблици.
		1.4.3	Разбиране на предимствата и ограниченията при криптиране.
2 Зловреден софтуер	2.1 Определение и функции	2.1.1	Разбиране на термина зловреден софтуер.
		2.1.2	Разпознаване на различни начини, по които зловредният софтуер може да се прикрие: троянец, руткит и задна врата (trojans, rootkits and back doors).
	2.2 Типове	2.2.1	Разпознаване на типовете инфекциозен зловреден софтуер и разбиране как работи той: вируси, червеи (viruses, worms).
		2.2.2	Разпознаване на типовете зловреден софтуер за кражба на данни, генериране/изнудване на печалба и разбиране как работят: рекламен, шпионски софтуер, ботнетове, софтуер за запаметяване на употребени клавиши и набиране на телефонни номера (adware, spyware, botnets, keystroke logging and diallers).
	2.3 Предпазване	2.3.1	Разбиране как работи антивирусният софтуер и какви са неговите ограничения.
		2.3.2	Сканиране на определени харддискове, папки, файлове с антивирусен софтуер. Задаване на график за сканиране на антивирусния софтуер.
		2.3.3	Разбиране на термина карантина и ефектите от поставяне на заразени/подозрителни файлове под карантина.

		2.3.4	Разбиране на важността от редовно софтуерно обновяване.
3 Сигурност на мрежата	3.1 Мрежи	3.1.1	Разбиране на термина мрежа (network) и разпознаване на най-често срещаните типове мрежа като: локална мрежа (LAN), глобална мрежа (WAN), виртуална лична мрежа (VPN)
		3.1.2	Разбиране на ролята на мрежовия администратор при удостоверяване (authentication), предоставяне на разрешение (authorisation) и отчитане (accounting) в мрежа.
		3.1.3	Разбиране на функциите и ограниченията на защитната стена.
	3.2 Мрежови връзки	3.2.1	Разпознаване на вариантите за свързване в мрежа като: кабелна и безжична (wireless) връзка.
		3.2.2	Разбиране, че свързването в мрежа има последици като: зловреден софтуер, непозволен достъп до данни, загуба на неприкосновеност.
	3.3 Сигурност при безжична връзка	3.3.1	Осъзнаване на важността от изискване на парола за защита на безжична връзка.
		3.3.2	Различаване на типовете защита на безжична връзка като: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC).
		3.3.3	Осведоменост за риска от употреба на незащитена безжична връзка – „подслушвачи“ (eavesdroppers) могат да получат достъп до нея.
		3.3.4	Свързване в защитена/незащитена безжична връзка.
	3.4 Контрол на Достъпа	3.4.1	Разбиране на нуждата от профил в мрежата и как се влиза в него чрез потребителско име и парола.
		3.4.2	Познаване на добрите практики при работа с пароли: не се споделят с никого, сменят се често, адекватна дължина и сложност.
		3.4.3	Определяне на основните биометрични техники за сигурност, използвани при контрол на достъпа: чрез пръстов отпечатък, сканиране на зеница.
4 Безопасна употреба на мрежата	4.1 Сърфиране в Интернет	4.1.1	Осведоменост за рисковете при определена онлайн активност – покупки и финансови транзакции се предприемат само в сигурни уеб страници (secure web pages).
		4.1.2	Идентифициране на сигурни уебсайтове чрез: https, символ-катинар (lock symbol).
		4.1.3	Осведоменост за понятието фарминг (pharming).
		4.1.4	Запознаване с термина дигитален сертификат (digital certificate). Потвърждаване на дигитален сертификат.

		4.1.5	Запознаване с термина еднократна парола (one-time password).
		4.1.6	Избор на подходящи настройки за включване/изключване на функция за автоматично довършване (autocomplete) и съхраняване (autosave) при попълване на електронни форми (form).
		4.1.7	Запознаване с термина бисквитка (cookie).
		4.1.8	Избор на подходящи настройки за позволяване или блокиране на бисквитки.
		4.1.9	Изтриване на лични данни от браузър като: история, кеширани интернет файлове (cached internet files), пароли, бисквитки, данни на автоматичното довършване.
		4.1.10	Разбиране на целите, функциите и типовете софтуер за контрол на съдържание като: софтуер за филтриране на интернет (filtering software), софтуер за родителски контрол (parental control software).
	4.2 Социални мрежи	4.2.1	Разбиране на важността от опазване на поверителна информация в социалните мрежи.
		4.2.2	Разбиране на нуждата от прилагане на правилни лични настройки на профил в социална мрежа.
		4.2.3	Разбиране на потенциални опасности при употреба на социални мрежи като: кибер тормоз (cyber bullying), набелязване на „жертви“ и сближаване с цел злоупотреба (grooming), подвеждане в заблуда (misleading), фалшиви самоличности (false identities), измамни съобщения и линкове (fraudulent links).
5 Комуникация	5.1 Електронна поща	5.1.1	Разбиране на целта на криптиране и декриптиране на електронна поща.
		5.1.2	Запознаване с термина дигитален сертификат.
		5.1.3	Създаване и добавяне на дигитален подпис (digital signature).
		5.1.4	Разбиране на възможността за получаване на измамни и непоискани писма (fraudulent and unsolicited e-mail).
		5.1.5	Запознаване с термина фишинг. Идентифициране на най-честите признаци за фишинг като: използване на имена на законни фирми и имена на хора, фалшиви уеб линкове.

		5.1.6	Осведоменост за опасностите от инфектиране на компютър със зловреден софтуер при отваряне на прикрепен файл в писмо, който съдържа макро или изпълнителен файл (.exe).
	5.2 Мигновени съобщения	5.2.1	Разбиране на термина мигновени съобщения (instant messaging) и употреба.
		5.2.2	Разбиране на слабите места в сигурността при употреба на мигновени съобщения като: зловреден софтуер, достъп през „задната врата“ (backdoor access), достъп до файлове.
		5.2.3	Разпознаване на методи за опазване на поверителността при употреба на мигновени съобщения като: криптиране, несподеляне на важна информация, ограничаване на споделянето на файлове.
6 Безопасно управление на данни	6.1 Създаване на резервно копие на данните	6.1.1	Разпознаване на начини за опазване на физическа сигурност на устройства чрез: използване на кабелни заключващи устройства, контрол на достъпа.
		6.1.2	Разбиране на важността от резервни копия в случай на загуба на информация; финансови отчети и уеб история и отметки (bookmarks).
		6.1.3	Установяване на процедура по създаване на резервно копие на информацията: редовно, по график, място на съхранение.
		6.1.4	Създаване на резервно копие на информация и данни.
		6.1.5	Възстановяване на резервно копие на информация и данни.
	6.2 Сигурно унищожаване на данни	6.2.1	Разбиране на необходимостта от перманентно изтриване на данни от харддиск и устройства.
		6.2.2	Различия между изтриване и унищожаване на данни (deleting and destroying).
		6.2.3	Определяне на най-честите методи за унищожаване на данни като: машинно раздробяване на физически документи (shredding), унищожаване на медия/харддиск, размагнитване (degaussing), използване на софтуер за унищожаване на данни.