ECDL Foundation

ECDL- ИТ Безбедност

Наставен план(Syllabus) Верзија 1.0

Модул 7–ИТ безбедност

Во модул 7 ИТ безбедност се наведени концепти и вештини кои се однесуваат на безбедност и користење на ИКТ во секојдневниот живот.Наставниот план опфаќа користење на релевантни техники и апликации за одржување на безебеднини конекции на мрежа, безбедно и сигурно користење на интернет, како и управување со податоци и информации на одговорен начин.

Цел на модули

Кандидатите би требало да:

- Да ги разберат клучните концепти кои се однесуваат на важноста за безбедноста на информациите и податоците, физичката сигурност, приватност и крадење на идентитетот
- Заштита на компјутер, уред или мрежа од злонамерни програми и неовластени пристапи на истите
- Да ги разберат разните врсти на мрежи, конекции и специфични прашања за компјутерска мрежа со вклучување на заштитен ѕид (firewall)
- Пребаруваат web страни и безбедно да комуницираат преку интернет
- Да ги разберат сигурносните прашања поврзани за комуникацијата, со вклучување e-mail и инстант пораки
- Да прават копија на податоците (back up), враќање на (restore) податоци на точен и безбеден начин и безбедно располага со податоците во уредот.

ПОДГЛАВЈЕ	ОБЛАСТ	ЗНАК	ЦЕЛ
1. Концепти на безбедности	*1.1Податоци*	1.1.1	Да прават разлика помеѓу податоци и информации.
		1.1.2	Да се разбере поимот сајбер криминал
		1.1.3	Да се разбере разлика помеѓу тернимот хакирање, кракување и етичко хакирање.
		1.1.4	Да се препознае закана на податоците како што се: пожар, поплава, војна и земјотрес.
		1.1.5	Да се препознае закана на податоците од страна на запослените, сервис провајдери и поединци од надворешно окружување.
	1.2 Важност на информации	1.2.1	Да се разбере важноста за заштита на личните податоци: крадење на идентитет и измама.
		1.2.2	Да се разбере причината за заштита на осетливите работни информации: кражба или злоупотреба на детали од клиенти и финансиски информации.
		1.2.3	Идентификивање на мерка за пречување на неовластени пристапи на податоци, како што се шифрирање (енкрипција) и лозинки.
		1.2.4	Да се разберат основни

			карактеристики на безбедност на иформации како што се: доверливост, интегритет и достапоност.
		1.2.5	Да се идентификуваат начини на заштита на податоци и приватност, контрола на пристап на податоци и сл. во вашата земја
		1.2.6	Да се разбере важноста на креирање и придржување кон обележјата и политиката на користење на ИКТ
	1.3 Лична безбедност	1.3.1	Да се разбере терминот на социјален инжињеринг и импликации како што се: собирање на информации, измама, пристап на системот на компјутерот.
ПОДГЛАВЈЕ	**ОБЛАСТ**	**ЗНАК**	**ЦЕЛ**
		1.3.2	Индентификување на методи од социјалниот инжињеринг како што се: телефонски разговори, phishing, ,, сурфање преку рамо"(shoulder surfing)
		1.3.3	Да се разбере значењето и импликациите на терминот крадење на идентитетот: личен,финансиски, работен и правен.
		1.3.4	Идентификување на методи кражба на идентитет како што се: information diving (копање по податоци), skimming(симнување на податоци од магнетна трака), pretexting (измислено сценарио)
	1.4 Безбедност на фајлови	1.4.1	Да се разберевклучување/исклучување макро наредби.
		1.4.2	Поставување на лозинки за фајлови како што се: документи, копресирани фајлови, табеласни калкулации.
		1.4.3	Да се разберат предностите и ограничувањето на шифрирањето (енкрипции).
2. Злонамерни програми	*2.1 Дефиниции и функции*	2.1.1	Да се разбере поимот злонамерен програм (malware).
		2.1.2	Да се препознаат различни врсти на прикривени злонамерни програми како што се: trojans, rootkits i back doors.
	2.2 Врсти	2.2.1	Да препознае врсти на злонамерни програми како што се вируси и црви.
		2.2.2	Да препознае врсти на кражба на податоци и злонамерни програми за изнуда како што се: adware (програми за огласување), spyware (шпиунски програми), botnets, keystroke logging i diallers (бирачи).
	2.3 Заштита	2.3.1	Да разбере начин на работа и ограничување на антивирусниот програм.

		2.3.2	Скенирање на специфични дискови (drives), фолдери, фајлови со користење на антивирусен програм. Закажете скенирање на антивирусната програма
		2.3.3	Да го разбере терминот „карантин“ и неговиот влијание на заразени/сомнителни фајлови.
		2.3.4	Да ја разбере важноста на редовното ажурирање на антивирусната програма.
3. Безбедност на мрежа	*3.1Мрежи*	3.1.1	Да го разбере терминот мрежа и да разбере врста на мрежи како што се: LAN, WAN i VPN.
		3.1.2	Да ја разбере улогата на администраторот за мрежа
		3.1.3	Да ја разбере функцијата и ограничувањето на заштитниот ѕид (firewall).
	3.2 Начин на поврзување на мрежа	3.2.1	Да препознае опција за поврзување на мрежа-по пат на кабел или безжично.
		3.2.2	Да разбере како поврзување на мрежа може да влијае на безбедноста: злонамерни програми, недозволен пристап на податоци, заштита на приватноста.
	3.3 Безбедност на безжични мрежи	3.3.1	Да препознае важноста на заштита на безжичните мрежи.
		3.3.2	Да препознае различни начини на заштита на безжичните мрежи како што се WEP, WPA, MAC.

ПОДГЛАВЈЕ	ОБЛАСТ	ЗНАК	ЦЕЛ
		3.3.3	Да се биде свесен дека користењето на незаштитени безжични мрежи можат да доведат до неовластени пристапи до вашите податоци.
		3.3.4	Пристап на заштитена/незаштитена безжична мрежа.
	3.4 Контрола на пристап	3.4.1	Да разбере потребата од налог на мрежа и пристап со користење на корисничко име и лозинка.
		3.4.2	Да ја разбере важноста и правилниот начин на креирање на лозинки – лозинката траба да содржи букви, броеви и знакови и сл, треба редовно да се менува, не треба да се дели со никого.
		3.4.3	Да се препознае сигурносната техника во контрола на пристап како што се: отисоци на прсите или скенирање на зеницата на око.
4. Сигурно користење на web пребарувач	*4.1 Web пребарувач*	4.1.1	Да разбере дека он лајн активностите, како што се купувањата или финансиските трансакции, се вршат преку сигурни web страници.
		4.1.2	Да се идентификуваат сигурни web страници: https, lock symbol и сл.

		4.1.3	Да разбере што се на сајбер напади
		4.1.4	Да го разбере терминот дигитален сертификат. Да се провери исправноста на дигиталниот сертификат
		4.1.5	Да го разбере терминот еднократна лозинка.
		4.1.6	Да се изберат правите подесувања за овозможување и оневозможување на автоматски внес и автоматско чување на податоци со пополнување на образец.
		4.1.7	Да го разбере терминот „колаче“ (cookie)
		4.1.8	Да се изберат правите подесувања за дозвола и блокирање на колачиња (cookie)
		4.1.9	Да се избришат личните податоци од web читачот како што е: историја на пребарување, кеширани интернет фајлови, колачиња, автоматско внесување на податоци.
		4.1.10	Да ја разбере суштината, функцијата и врсти на програми за конторла на содржини: програм за интернет филтрирање, програм за родителска контрола.
	4.2 Друштвени мрежи	4.2.1	Да разбере зошто не треба да се поставуваат лични и приватни податоци на друштвените мрежи.
		4.2.2	Да разбере дека е потребно да се применат подесувања што одговараат на приватност на налог на општествените мрежи.
		4.2.3	Да ги разбере потенцијалните опасности при користење на друштвени мрежи како што е: вознемирување преку интернет, лажен идентитет, заразени линкови или пораки и сл.
5. Комуникации	*5.1 E-mail пораки(Електронска пошта)*	5.1.1	Да ја разбере поентата нашифрирањето (енкрипција) и дешифрирањето (decrypting) на e-mail пораки.
		5.1.2	Да го разбере терминот дигитален подпис.
		5.1.3	Да направи и додаде дигитален потпис.
		5.1.4	Да биде свесен за можностите од лажни примања и нежелни пораки.
		5.1.5	Да го разбере терминот и карактеристиките Phishinga(обид за превземање на информации) како што се користење на имиња на угледни компании, луѓе и лажни линкови.
		5.1.6	Да се биде свесен за потенцијалните опасности со

				отварање на прилози кои содржат макро наредби или извршни фајлови.
		5.2 Инстант пораки	5.2.1	Да го разбере терминот и суштината на IM – Инстант порака.
			5.2.2	Да разбере потенцијала опасност при размена на инстант порака како што се: злонамерни програми (malware), backdoor пристап, пристап на фајлови и сл.
			5.2.3	Да препознае методи за обезбедување на поверливост при размена на ИМ коко што се:шифрирање (енкрипција), не објавување на важни информации и ограничување во делење на фајлови.
6.	**Управување со сигурноста на податоци**	*6.1 Безбедност и правење на сигурносни копии на податоци*	6.1.1	Да препознае начини за обезбедување на физика сигурност на уреди – користење на брава за каблови ,контрола на пристап и сл.
			6.1.2	Да препознае важноста и процедура за правење на копии на податоци во случај на губење на истите, финансиски извештаи, пребарување во историја и сл.
			6.1.3	Да ги препознае карактеристиките на правење на копии на податоци како што се: фрекфентрност, локација за чување на податоци, закажување правење на копии.
			6.1.4	Правење на сигурносни копии на податоци.
		6.2 Трајно уништување на податоци	6.2.1	Да разбере причина за трајно бришење на податоци од дискови или уреди.
			6.2.2	Да разликува бришење и трајно уништување на податоци.
			6.2.3	Да идентификуа методи за трајно уништување на податоци како што се: користење на уништувач за хартија, уништување на дискови/медии, размагнетисување,користење на помошен програм за уништување на податоци.