ECDL Foundation

ECDL / ICDL Osa 12 - IT Turvalisus

Õppekava v.1.0

Tingimused
Kuigi ECDL Foundation on hoolikalt käesoleva dokumendi koostanud ja kontrollinud enne avaldamist, ei garanteeri ECDL Foundation, kirjastaja, teabe täielikkust, samuti ei vastuta ECDL Foundation võimalike vigade, väljajätmiste, ebatäpsuste tulmusel sündivast võimalikust kahjust käesoleva dokumendi juhiste või soovituste järgimisel . ECDL Foundation ed võib teha dokumendis muutusi omal äranägemisel ja igal ajal ilma ette teatamata. Dokumendi IT Security ametlik versioon on avaldatud ECDL Foundation kodulehel: www.ecdl.org

ECDL / ICDL Osa 12 - IT Turvalisus

Dokument sisaldab ECDL / ICDL Osa 12 - IT Turvalisus üksikasjalikku õppekava. Õppekava kirjeldab õpitulemuste kaudu teadmisi ja oskusi, mida eksaminand ECDL / ICDL Osa 12 - IT Turvalisus läbimisel peab omandama. Õppekava on aluseks ka selle osa teooriale ja praktikale eksami sooritamiseks.

Osa eesmärk

ECDL / ICDL Osa 12 - IT Turvalisus annab eksaminandile üldist arusaamise IKT turvalise kasutamise põhimõtetest igapäevaelus. Eksaminand peab oskama kasutada sobivaid võtteid ja rakendusi võrguühenduste turvamiseks, kasutama Internetti kaitstult ja turvaliselt, ja hallata andmeid ja teavet asjakohaselt. Tüüpiliselt on eksaminand varustatud teadmistega turvaliseks tööks IKT vallas ja ta suudab maandada enamlevinud turvariske IKT kasutamisel.

Eksaminand peab:
• mõistma tähtsamaid info turvamise, andmete füüsilise turvalisuse ja andmete füüsilise turvalisuse, privaatsuse ja identiteedi vargusega seotud põhimõisteid
• suutma kaitsta arvutit, seadet või võrku õelvara ja loata juurdepääsu eest
• tundma võrkude tüüpe, ühenduste tüüpe ja võrguspetsiifilisi probleeme, sealhulgas tulemüüre
• oskama sirvida World Wide Web'is, suhelda internetis turvaliselt
• mõistma side, sealhulgas e-posti ja sõnumivahetuse turvaküsimusi
• oskama varundada ja taastada andmeid sobival viisil ja ja turvaliselt ning ohutult hävitada mittevajalikke andmeid ja utiliseerida seadmeid.

Peatükk	Valdkond	Viide	Teema
12.1 Turvalisuse põhimõisted	*12.1.1 Ohud andmetele*	12.1.1.1	Eristada andmeid ja teavet. .
		12.1.1.2	Mõista küberkuritegevuse terminit.
		12.1.1.3	Mõista erinevust häkkimise, andmete hävitamise ja eetilise häkkimise vahel.
		12.1.1.4	Teadvustada vääramatu jõu (force majeure) ohte andmetele, näiteks: tulekahju, üleujutus, sõda, maavärin.
		12.1.1.5	Teadvustada ohte andmetele,: oma töötajate, teenusepakkuja töötajate ja väliste isikute poolt.
	12.1.2 Info väärtus	12.1.2.1	Mõista põhjusi kaitsta isikuandmeid, nagu: identiteedivargus, pettus.
		12.1.2.2	Mõista põhjusi miks kaitsta tundlikku äriteavet, nagu: kliendi andmete, finantsinfo varguse või väärkasutamise vältimine.

Peatükk	Valdkond	Viide	Teema
		12.1.2.3	Meetmed volitamatu juurdepääsu vältimiseks andmetele, nagu: krüpteering, paroolid.
		12.1.2.4	Mõista infoturbe põhitermineid: terviklus, konfidentsiaalsus, käideldavus.
		12.1.2.5	Peamised andmete ja eraelu puutumatuse kaitse, säilitamise ja kontrollimise nõuded Eestis.
		12.1.2.6	Mõista kui tähtis on luua ja järgida instruktsioone ja reegleid IKT kasutamisel. .
	12.1.3 Isiku turvalisus	12.1.3.1	Mõiste *social engineering* ja selle mõju, nagu: teabe kogumine, pettused, juurdepääs arvutile.
		12.1.3.2	*Social engineering* meetodid,: telefonikõned, phishing, üle õla vaatamine.
		12.1.3.3	Mõiste identiteedivargus ja selle mõju: isiku-, finantsiline, äriline, õiguslik.
		12.1.3.4	Identiteedivarguse meetodid : info taastamine (information diving), riibe (skimming), ettekääne (pretexting).
	12.1.4 Failide Turvalisus	12.1.4.1	Mõista makrode turvaseadete lubamise / keelamise tulemusi.
		12.1.4.2	Määrata parool failidele: dokumendid, pakitud failid, arvutustabeleid.
		12.1.4.3	Mõista krüpteerimise eeliseid ja piiranguid.
12.2 Pahavara	*12.2.1 Definitsioon ja eesmärk*	12.2.1.1	Mõista õelvara terminit.
		12.2.1.2	Tunda erinevaid võimalusi, kuidas pahavara võib peita näiteks: troojad, rootkit ja tagauksed.
	12.2.2 Types	12.2.2.1	Tunda nakkav õelvara tüüpe ja mõista, kuidas nad töötavad, näiteks: viirused, ussviirused.

Peatükk	Valdkond	Viide	Teema
		12.2.2.2	Tunda andmevarguse tüüpe, raha teeniva / väljapressimise õelvara ja mõista, kuidas nad töötavad: reklaamvara, nuhkvara, botnet, klahvivajutuse salvestamine ja väljahelistamine.
	12.2.3 Kaitse	12.2.3.1	Mõista, kuidas viirusetõrje tarkvara töötab ja selle piiranguid.
		12.2.3.2	Skanneerida konkreetseid kettaid, kaustu, faile viirusetõrje tarkvaraga. Viirusetõrjega ajastatud skaneerimine.
		12.2.3.3	Mõistest karantiin ja vajadusest karantiinida nakatunud või kahtlasi faile.
		12.2.3.4	Mõista tarkvarauuenduste allalaadimise ja installeerimise tähtsust, viirusetõrje uuendamist.
12.3 Võrguturve	*12.3.1 Võrgud*	12.3.1.1	Arvutivõrgu mõiste ja võrgutüübid: kohtvõrk (LAN), laivõrk (WAN), virtuaalne kohtvõrk (VPN).
		12.3.1.2	Mõista võrguadministraatori rolli võrgus autentimise, autoriseerimise ja ressursikasutamise juhtimisel.
		12.3.1.3	Tunda tulemüüri funktsioone ja piiranguid.
	12.3.2 Võrgu-ühendused	12.3.2.1	Tunda võrku ühendamise võimalusi: kaabel, traadita võrk.
		12.3.2.2	Mõista, kuidas võrku ühendamine mõjutab turvalisust: pahavara, volitamata juurdepääs andmetele, privaatsuse säilitamine.
	12.3.3 Traadita võrgu turve	12.3.3.1	Tunnustada parooli kasutamis nõudmist kaitstes traadita võrguühendust.
		12.3.3.2	Tunda erinevat tüüpi traadita võrgu turvalisuse kaitse protokolle: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC).

Peatükk	Valdkond	Viide	Teema
		12.3.3.3	Olla teadlik, et kaitsmata traadita võrk võimaldab välisel kasutajal juurdepääsu andmetele.
		12.3.3.4	Ühendamine kaitstud / kaitsmata traadita võrku.
	12.3.4 Juurdepääsu piiramine	12.3.4.1	Mõista võrgukonto kasutamise eesmärki ja kuidas seda kasutada kasutajanime ja parooliga.
		12.3.4.2	Tunda hea parooli reegleid, nagu: ei jaga paroole, muuta neid regulaarselt, piisav parooli pikkus, sobivalt tähti, numbreid ja erimärke lisatud.
		12.3.4.3	Üldised biomeetrilise turvalisuse võtted juurdepääsu kontrolliks nagu: sõrmejälje, silmaiirise skanneerimine.
12.4 Turvaline veebikasutus	*12.4.1 Veebi-lehitsemine*	12.4.1.1	Tuleb olla teadlik, et teatud tegevused veebis (ostmine, finantstehingud) tuleks sooritada ainult turvalistel veebilehtedel.
		12.4.1.2	Määratleda turvalisele veebisaidile omased tunnused: https, luku sümbol.
		12.4.1.3	Teada ümbersuunamise võimalusest (*pharming*).
		12.4.1.4	Mõiste digitaalne sertifikaat. Digitaalse sertifikaadi kontrollimine.
		12.4.1.5	Mõistest ühekordne parool.
		12.4.1.6	Kuidas valida välja sobivad seaded väljade automaatseks täitmiseks, automaatseks salvestamiseks veebivormide täitmisel.
		12.4.1.7	Küpsise (*cookie*) mõistest.
		12.4.1.8	Select appropriate settings for allowing, blocking cookies Kuidas valida sobivad seaded mis võimaldavad lubada või blokeerida küpsiseid.
		12.4.1.9	Isiklike andmete kustutamine: sirvimise ajalugu, puhverdatud interneti failid, paroolid, küpsised, automaatselt salvestatud andmed.

Peatükk	Valdkond	Viide	Teema
		12.4.1.10	Mõista sisukontrolli tarkvara eesmärki, funktsiooni ja tüüpe: interneti filtreerimistarkvara, vanema- kontrolli tarkvara.
	12.4.2 Sotsiaal-võrgustikud	12.4.2.1	Mõista, kui tähtis on mitte avaldada konfidentsiaalset teavet sotsiaalvõrgustikes.
		12.4.2.2	Be aware of the need to apply appropriate social networking account privacy settings.
		12.4.2.3	Teada võimalikke ohte võrgusuhtlusel: küberkiusamine, kommionud, eksitava/ ohtliku teabe andmine, vale-identiteet, valed lingid ja sõnumid. .
12.5 Sidevahendid	*12.5.1 E-post*	12.5.1.1	Tunda krüptitud,krüptimata e-posti.eesmärke.
		12.5.1.2	Digiallkirja mõiste.
		12.5.1.3	Luua ja lisada digiallkiri.
		12.5.1.4	Olla teadlik võimalusest saada petukirju ja soovimatut e-posti (rämpsposti).
		12.5.1.5	Mõistest andmepüük (phishing). Üldised tunnused nagu: reaalsete ettevõtete ja inimeste nimed, valede veebilinkide kasutamine.
		12.5.1.6	Teada, et on võimalik oht nakatada arvuti pahavaraga avades e-kirja manuse, mis sisaldab makrot või käivitatavat faili.
	12.5.2 Sõnumi-vahetus	12.5.2.1	Sõnumivahetus (IM) ja selle kasutusviisid.
		12.5.2.2	Sõnumivahetuse haavatavusi: pahavara, tagauks, juurdepääs failidele.
		12.5.2.3	Sõnumivahetuse krüpteerimine piirangud olulise teabe edastamisel, failide ühiskasutusel.
12.6 Turvaline andmehoid	*12.6.1 Andmekaitse ja varundus*	12.6.1.1	Kuidas tagada füüsilist turvalisust seadmetele nagu: logiseadmete asukoht ja andmed, kaablilukud, juurdepääsu piiramine.

Peatükk	Valdkond	Viide	Teema
		12.6.1.2	Teada varundus- ja taastevõtteid andmete kadumisel, raamatupidamisinfo, veebi järjehoidjate / ajaloo puhul.
		12.6.1.3	Nimetada varunduse omadusi: regulaarsus / sagedus, ajastus, ladustamise asukoht.
		12.6.1.4	Varundamine.
		12.6.1.5	Andmete taastamine ja valideerimine.
	12.6.2 Turvaline andmete hävitamine	12.6.2.1	Vajadus jäädavalt kustutada andmeid ketastel või seadmetes.
		12.6.2.2	Kuidas eristada andmete kustutamist ja jäädavalt hävitamist.
		12.6.2.3	Jäädavalt hävitamise meetodid: ribastamine, meedia hävitamine, magneetimine, andmete hävitamise lteenused.