

Ka ilaalinta shabakadaha (networks) khataraha amniga



Computing

Unit Hordhaca amniga internetka (cybersecurity)

Natiijo

Waxaan barbardhigi karaa khataraha amniga nidaamka kombuyuutarka oo waxaan soo jeedin karaa tallaabooyin ilaalino.

Erayada muhiimka ah

Amniga internetka (cybersecurity)

Ilaalinta nidaamyada kombuyuutarka khataraha

Firewall

Nidaam shaandheeya taraafikada shabakada si uu uga ilaaliyo qulqulka xogta ee aan la oggolaan ee gudaha ama dibadda shabakada

Ka ilaalinta shabakadaha (networks) khataraha amniga



Barbar dhig khataraha amniga



Sharax sida nidaamyada iyo shabakadaha loo ilaalin karo

Khatarta internetku (cyber threat) waa wax dhibi kara kombuyuutarkaaga ama siin kara helitaanka xogtaada shakhsiyeed.

Waa daciifnimo la heli karo oo la isticmaali karo.



Amniga internetka (cybersecurity) waa ilaalinta nidaamyada kombuyuutarka ama shabakadaha khataraha jira iyo kuwa cusub.





Layla

Maxay iskuulku u baahan yahay inuu ka ilaaliyo weerarrada internetka (cyber attacks)?

Waxay u baahan yihiin inay ilaaliyaan wax kasta oo si dijitaal ah loo kaydiyo. Tusaale ahaan, macluumaadka shakhsiyeed ee ardayda iyo macallimiinta, erayada sirta ah (passwords) iyo sawirada.



Cali

Iskuulku waxa uu samayn karaa falanqeyn khatar (risk analysis) si uu u qiimeeyo khataraha ay u badan tahay inay soo gaadhaan xogtooda dijitaalka ah, sida

- hackers (hackers)
- malware (malware)
- phishing (phishing)
- shilalka iyo qaladaadka
- masiibooyinka dabiiciga ah
- social engineering (social engineering)



Ka dib markii la aqoonsaday khataraha suurtagalka ah, dugsigu wuxuu eegaa daciifnimada. Tusaale ahaan:

- Ma fudud yahay in la qiyaaso erayada sirta ah (passwords)?
- Ma cusub yahay software-ka (software)?
- Dadku ma gujiyaan xiriiriyeyaasha (links) ka yimid dad aan la aqoon?



Ka dib markii la aqoonsaday khataraha iyo daciifnimada, dugsigu wuxuu tixgeliyaa inta ay u badan tahay inay dhacdo iyo saamaynta ay yeelan karto haddii khatartu guulaysato.



Jaantuska falanqaynta khatarta (risk analysis matrix) ayaa loo isticmaalaa in lagu qiimeeyo khataraha cybersecurity-ka. Wuxuu kuu ogolaanayaa inaad isbarbardhigto khataraha midba midka kale.

		saamaynta (impact)			
		masiibo	sare	dhexdhexaad	yar
ixtimaalka (probability)	ku dhawaad hubaal	aad u sare	aad u sarreeya	sarreeya	dhexdhexaad
	sugan	aad u sarreeya	sarreeya	dhexdhexaad	dhexdhexaad
	dhexdhexaad	aad u sarreeya	sarreeya	dhexdhexaad	hooseeya
	aan suganayn	sarreeya	dhexdhexaad	dhexdhexaad	hooseeya
	naadir	dhexdhexaad	dhexdhexaad	hooseeya	hooseeya



Layla

Xagee ku yaallaa khatarta uu hacker-ku si aan la fasaxin u galo nidaamka dugsiga?

Waa kuxiran. Marka hore, ka fikir sida ay u badan tahay in dugsigaaga la hack-garo. Kadibna ka fikir saamaynta (impact) ay arrintaasi ku yeelan karto dugsigaaga haddii ay dhacdo.



Cali



Layla

Marka, waxaad go'aamin kartaa halka ay ku habboon tahay shaxda falanqaynta khatarta (risk analysis matrix)?

Haa, dugsigastaa waa kala duwan yihiin! Boosku wuxuu kuxiranyahay dugsigu inuu aqoonsado waxyaabaha nugul (vulnerabilities) ee la isticmaali karo.



Cali

Maxay shirkad u isticmaali kartaa si ay u falanjeeyso oo u barbardhigto khataraha amniga internetka (cybersecurity threats)?

a

garaaf khatar (risk graph)

b

falanqayn khatar (risk analysis)



c

falanqayn khatar (threat analysis)

Dugsigani wuxuu dhigayaa hacker-ka ixtimaal dhexdhexaad ah (moderate probability) iyo saamaynta (impact) masiibo (disaster).

saamaynta (impact)

ixtimaalka (probability)

	masiibo (disaster)	sare (high)	dhexdhexaad	yar
ku dhawaad hubaal	aad u sarreeya	aad u sarreeya	sarreeya	dhexdhexaad
sugan	aad u sarreeya	sarreeya	dhexdhexaad	dhexdhexaad
dhexdhexaad	aad u sarreeya	sarreeya	dhexdhexaad	hooseeya
aan suganayn	sarreeya	dhexdhexaad	dhexdhexaad	hooseeya
dhif	dhexdhexaad	dhexdhexaad	hoose	hoose

Dugsi ayaa kaa codsaday inaad dhamaystirto qiimeyn khatar (risk assessment) oo ku saabsan khataraha amniga internetka (cybersecurity).

Dugsigu wuxuu ku yaalaa deegaan miyi ah oo ku yaala England.

Waxay u oggolaadaan ardayda iyo macallimiinta inay isticmaalaan iimaylka (email), abuuraan erayada sirta ah (passwords), macallimiintuna waxay soo dejisan karaan (download) waxyaabo cusub ama software.

Macallimiinta iyo ardayduba waxay isticmaali karaan aaladaha USB (USB devices) si ay ugu shubaan (load) oo u kaydiyaan (store) faylasha.

Shaqaalaha iyo ardayda dugsiga ayaa dhawaan la baray khiyaamada iimaylka (phishing) iyo inaysan gujin (click) linkiyada ku jira iimaylka.

Go'aami heerka shaxda falanqaynta khatarta (risk analysis matrix) ee khataraha soo socda.

Waa maxay khatartu?	Heerka shaxda khatarta (Risk matrix level)
hackers	
malware	
phishing	
qaladaadyo shil ah (accidental mistakes)	
masiibooyin dabiici ah (natural disasters)	
farsamada bulshada (social engineering)	

Go'aami heerka shaxda falanqaynta khatarta (risk analysis matrix) ee khatarahan soo socda. Jawaabahaagu way ka duwanaan karaan.

Waa maxay khatartu?	Heerka shaxda khatarta (risk matrix level)
hackers	aad u sarreeya
malware	aad u sarreeya
phishing	sarreeya
khaladaad shil ah	sarreeya
masiibooyin dabiici ah	hooseeya
farsamada bulshada (social engineering)	dhexdhexaad

Ka ilaalinta shabakadaha khataraha amniga



Isbarbardhig khataraha amniga



Sharax sida nidaamyada iyo shabakadaha loo ilaalin karo

Shirkadaha iyo ururradu waxay raacaan CIA Triad.

Waa mabda'a asaasiga ah ee amniga internetka (cybersecurity).



Qarsoodi (Confidentiality) – ilaalinta xogta inay helaan dad aan fasax lahayn.

Daacadnimo (Integrity) – hubinta in xogtu sax tahay oo aan la beddelin.

Helitaan (Availability) – hubinta in xogta ama nidaamyada la heli karo marka loo baahdo.



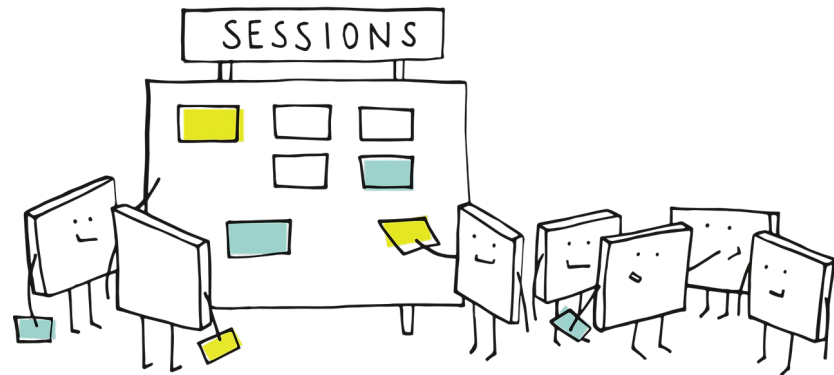
Weligaa ma samayn kartid nidaam 100% ammaan ah oo ka soo horjeeda weeraryahannada.

Laakiin waxaad samayn kartaa tallaabooyin adag si ay u adkaato weeraryahannada, si ay uga dhici karaan oo ay u helaan bartilmaameed fudud.



Tababarka joogtada ah wuxuu muhiim u yahay qof kasta oo isticmaala nidaamka si loo yareeyo qaladaadka.

Tusaale ahaan, ogaanshaha xeerarka erayga sirta ah (password) iyo inaan la gujin linkiyada shakiga leh.



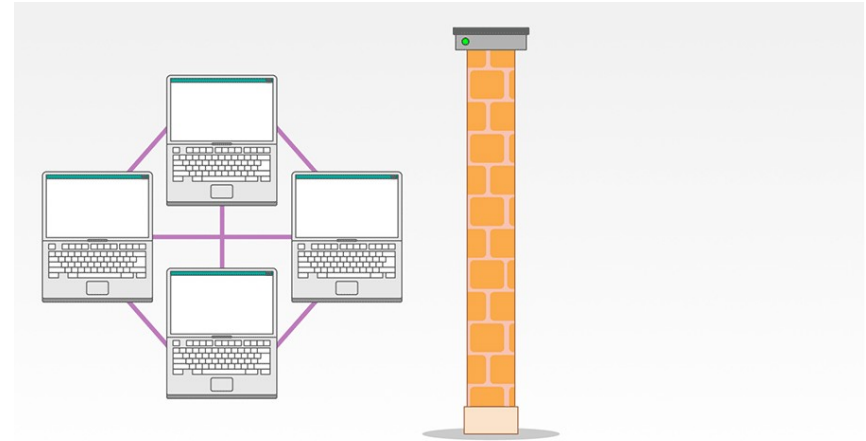
Dab-demiska (Firewall) wuxuu hubiyaa taraafikada shabakadda soo gasha iyo baxda.

Wuxuu baaraa xogta si loo hubiyo inaysan ku jirin wax shar ah oo uu raaco xeerarka shabakadda.



Tusaale ahaan:

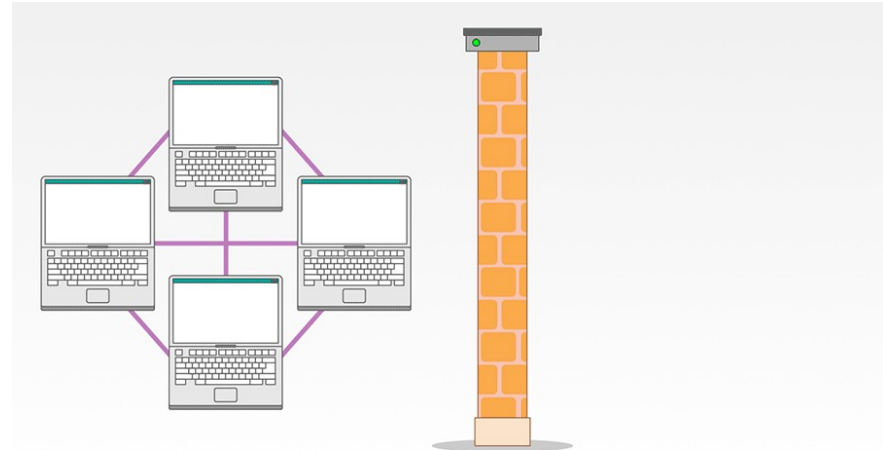
Ardaygu wuxuu isku dayaa inuu isticmaalo shabakad buuxda ciyaaraha bilaashka ah. Xeerarka shabakadda ayaa loo dejiyay inay diidaan tan, dab-demiskuna wuxuu joojiyaa ardayga inuu galo shabakadda.



Dab-demisku (Firewalls) wuxuu isticmaalaa sifeynta ku salaysan xeer (rule-based filtering).

Xirmooyinka xogta (Data packets) waa la baaraa iyadoo la eegayo xeerarka si loo go'aamiyo inay geli karaan ama ka bixi karaan shabakadda.

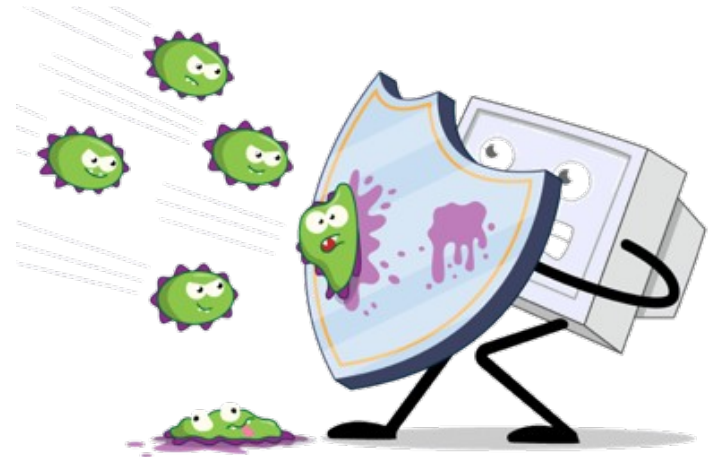
Dab-demiska (Firewall) wuxuu baaraa cinwaannada IP, nambarada port-ka, iyo borotokoolka (protocols).



Anti-malware waa software (barnaamij) oo baara fayl kasta oo awood u leh inuu fuliyo code (koodh).

Anti-malware waxay leedahay liis qeexid (definitions) — taxane code — oo la og yahay inay yihiin kuwo waxyeello leh.

Haddii code-ka faylkaagu uu u dhigma qeexidda, faylasha waa la karantiilay (quarantine).



Auto-updates waa halka software si otomaatig ah u baaro cusbooneysiin (updates) diyaar ah.

Haddii cusbooneysiin diyaar ah ay jirto, software-ku wuxuu uga digi doonaa isticmaalaha ama wuxuu si otomaatig ah ugu rakibi doonaa.

Software-kan badanaa wuxuu ku jiraa nidaamka hawlgalka (operating system).

Software update v.12.6

**A software update is available
and ready to install**

Install Now

Later

Details

Run mise been?

Firewall wuxuu baara dhammaan taraafikada shabakada ee soo gasha iyo kuwa baxa.



Run



Been

Wuxuu baara xogta si loo hubiyo inaysan ku jirin wax waxyeello leh iyo inay raacdo xeerarka shabakadu dejiso.

Xaqiijinta isticmaalaha (user authentication) waxay ka caawisaa ilaalinta nidaamyada ka dhanka ah gelitaanka aan la oggolaayn. Tan waxaa ka mid ah:

- ereyada sirta ah ee ammaanka leh (secure passwords)
- tirada ugu badan ee isku dayga gelitaanka ka hor inta aan akoonka la xirin

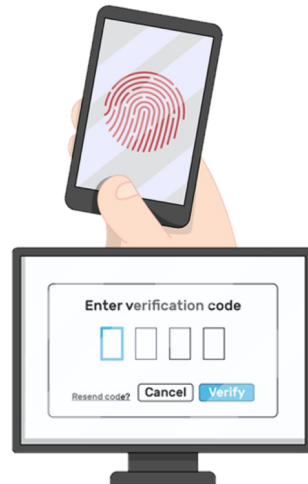


CAPTCHA – aqoonsashada sawirro gaar ah oo ku jira saf, ama qor waxa aad ku aragto muuqaal qalloocan.



Biometrics – aqoonsiga faraha iyo wejiga.

Xaqiijin laba-cabbir ah (2FA) – lambar ayaa loo diraa qalab ama iimayl kale.





Caasha

Ma siin kartaa isticmaalayaal kala duwan xuquuq gelitaan kala duwan?



Haa, waxaad siin kartaa qaar isticmaalayaal gelitaan drives-ka shabakada gaarka ah, dejinta ruqsadaha faylasha si ay u akhriyaan/qoraan oo keliya, iyo xaddidista gelitaanka daabacayaasha, software-ka ama websaytyada.



Nuur



Saciid

Ma doortaa hal tallaabo oo ammaan (security measure) si aad u ilaaliso nidaamka ama shabakadda?

Maya, waxaad doortaa inta aad u baahan tahay si aad u ilaaliso nidaamka ama shabakadda. Tallaabooyinka ammaanka oo badan, ayaa ilaalintu ka fiicnaanaysa.



Axmed



Isra

Ma joojisaa isticmaalka tallaabooyinka ammaanka dhammaan weerarrada internetka (cyber attacks)?

Maya, khataro cusub iyo farsamooyin horumarsan ayaa had iyo jeer la soo saaraa, waxayna mararka qaar ka gudbi karaan xitaa difaacyada ugu wanaagsan.



Suad

Kuwee ka mid ah kuwan soo socda ayaa tusaale u ah xaqiijinta isticmaalaha (user authentication)?

a

biometrics (biometrics)



b

ereyada sirta ah ee ammaanka ah (secure passwords)



c

cusboonaysiinta software-ka otomaatiga ah (software auto-updates)

1) Sharax sida iskuulku u ilaalin karo nidaamyadiisa khatar kasta oo ku jirta jaantuska hoose.

Waa maxay khatartu?	Tallaabooyinka ammaanka
hackers (hackers)	
malware (malware)	

1) Aqoonso sida iskuulku u ilaalin karo nidaamyadiisa khatar kasta oo ku jira shaxda hoose.

Waa maxay khatartu?	Tallaabooyinka amniga
hackers	firewall, laba-caddayn (two-factor authentication), erayada sirta ah ee ammaanka, biometrics, tirada ugu badan ee isku dayga gelitaanka
malware	anti-malware, firewall

2) Iskuulkaagu wuxuu u baahan yahay inuu hubiyo amnigiisa internetka. Waa maxay meelaha muhiimka ah ee ay diiradda saaraan si ay u ilaaliyaan kombuyuutarradooda iyo shabakadooda khataraha internetka?

2) Iskuulkaagu wuxuu u baahan yahay inuu hubiyo amnigiisa internetka. Waa maxay meelaha muhiimka ah ee ay diiradda saaraan si ay u ilaaliyaan kombuyuutarradooda iyo shabakadooda khataraha internetka?

Waa inay hubiyaan in firewall-ku shaqeynayo oo software-ka anti-malware-ka la rakibay. Had iyo jeer hubi in cusboonaysiinta software-ka la dhammeeyo. Hubi cidda ay heli karto waxa nidaamyada ku jira oo tixgeli xaddidista gelitaanka. Hubi in erayada sirta ah ee ammaanka la isticmaalayo oo xaddid tirada isku dayga gelitaanka. Fiiri ku darista laba-caddayn (two-factor authentication) ama biometrics sida lakab dheeri ah oo ammaan ah loogu talagalay isticmaalayaasha gelaya akoonnada.

Amniga internetka (Cybersecurity) waa sida aad u ilaalin karto nidaamyada kombuyuutarka khataraha internetka. Waxaad aqoonsan kartaa khataraha adoo dhammeystiray falanqaynta khatarta oo meel mariya habab lagu ilaaliyo nidaamyada iyo shabakadda.

Waxaa jira siyaabo badan oo lagu ilaaliyo nidaamyada iyo shabakadaha, oo ay ku jiraan firewalls, kuwaas oo baara dhammaan taraafikada shabakadda ee soo gala iyo kuwa baxa khataraha.

Ka warqabka khataraha amniga internetka iyo tallaabooyinka amniga waxay kaa caawin karaan joojinta weerarrada internetka.