Instaloni programe Anti-virus

Viruset dhe trojanët janë të dizajnuar për të infektuar kompjuterin ose për të marrë të dhënat nga kompjuteri. Viruset janë duke u bërë më të komplikuar dhe të ndërlikuar çdo vit. Nëse ju jeni të lidhur në internet apo jo, është gjithmonë mirë që të keni një program antivirus të instaluar në PC tuaj.

Instaloni update (përditësimet) e Windowsit

'Windows Update' është një shërbim që ofron Microsoft dhe kjo e lejon kompjuterin tuaj të qëndrojë i përditësuar dhe larg kërcënimeve të sigurisë si 'malware' dhe komponenteve të tjera të dëmshme. Vizitoni Windows Update për të përditësuar kompjuterin tuaj. Microsoft njofton për software updates (rifreskime të programeve) që janë projektuar për të zgjidhur kërcënimet e sigurisë. Të gjitha rifreskimet kritike (të rëndësishme) që janë FALAS duhet të shkarkohen dhe instalohen. Për të instaluar 'update' përcillni instruksionet:

- Klikoni në ikonën 'start/windows'
- Shkoni në 'All Programs'
- Zgjidhni 'Windows Update'
- Instaloni të gjitha update (përditësimet) kritike
- Ju mund të zgjidhni opsionin për instalim automatik të update (përditësimeve)

Instaloni firewall (mur mbrojtës)

'Firewall' ndihmon në filtrimin e trafikut në internet, kështu programe të dëmshme dhe hakerë nuk kanë qasje në kompjuterë. Pothuajse të gjitha paketat e sigurisë në internet kanë një firewall të ndërtuar në to. Windows XP, Vista dhe 7 brenda tyre përmbajnë firewall-in.

Instaloni vegla për largimin e programeve spyware/malware

Programet Spyware dhe malware janë të dizajnuara për të vjedhur fjalëkalime, vjedhje të identitetit, dhe për të krijuar pop-ups (dritare kërcyese që mbulojnë dritaret tjera). Malware do të infektojnë kompjuterët me virus dhe trojanë.

Instaloni programe për kontroll prindëror

Me këtë, prindërit mund të kufizojnë qasjen në Windows, të bllokojnë faqet e caktuara të internetit dhe të kufizojnë hyrjen në funksione të tilla si Control Panel, dokumente dhe shumë më tepër.

Instaloni një browser (shfletues interneti) të dytë të Interentit

Viruset dhe spyware shpesh kanë synim Internet Explorerin. Kur kompjuteri infektohet me malware ose viruse ata janë të projektuar për të mbajtur Internet Explorerin jashtë qasjes në internet. Instalimi i një browseri të dytë si: Firefox, Chrome, Safari ose Opera do të lejojë qasje në internet për të larguar viruset.

Çaktivizoni Java Script

Për të sulmuar PC viruset, malware dhe spyware gjithnjë e më shumë janë duke përdorur Java Script. Ndryshoni në settings të browserit (kërkoni që t'ju pyes para se të veprojë JavaScript) ose çaktivizoni JavaScript.

Krijoni Backup (duplikim) të dokumenteve

Krijoni një kopje rezervë të dokumenteve të rëndësishme në kompjuterin tuaj. Ju mund të krijoni një kopje rezervë të dokumenteve duke përdorur një hard disk të jashtëm – External Hard Drive, Flash Drive – USB ose të regjistroheni për një shërbim të duplikimit dhe ruajtjes online si: Dropbox,

Mozy, Gdrive, etj. Duplikimi është mirë të bëhet një herë në javë. Mënyra më e mirë për të bërë backup kompjuterin tuaj është online sepse informacionet ruhen përgjithmonë.

Mos instaloni programe të pasigurta nga interneti (pop-up)

Interneti është plotë uebfaqe të dizajnuara për të shkarkuar spyware dhe viruse.

Në ekranin tuaj mund të paraqitet një pop-up ku kërkohet që ju të instaloni një lojë apo diçka që duket argëtuese, por shumica e këtyre programeve nuk janë vërtetë të tilla dhe përmbajnë malware, spyware ose viruse. Nëse ju merrni rastësisht një pop-up nga një faqe interneti ku kërkohet që ju të instaloni diçka thoni "JO".

Kurrë mos hapni një attachment (shtojcë) e-mail nga dikush që ju nuk e njihni

Pothuajse të gjithë kompjuterët infektohen me viruse nëpërmjet email attachment (shtojcat). Nëse ju merrni një email që ka një (shtojcë) ku si subjekt ka diçka që tërheqë vëmendjen tuaj dhe vjen nga dikush që ju nuk e njihni MOS klikoni mbi të. Fshijeni email-in menjëherë.

Krijoni fjalëkalim të sigurt

Gjatë krijimit të një fjalëkalimi nuk duhet përdorur emrin, mbiemrin apo fjalë të përgjithshme. Preferohet që fjalëkalimi të jetë 8-14 karaktere i gjatë, i përbërë nga numra, shkronja të vogla e të mëdha, dhe simbole të veçanta. Këtu janë disa shembuj të fjalëkalimeve të forta. Kurrë mos i ndani fjalëkalimet me të tjerët. Mos e përdorni të njëjtin fjalëkalim në të gjitha faqet. Nëse është vjedhur, të gjitha informatat që i mbron ai fjalëkalim janë në rrezik.

Fjalëkalim i dobët	Fjalëkalim i mirë
Dritan1	driT@n1
Mrika	mr!c@Aa
America	Am&r1c@

Mbani të sigurt rrjetën e Wireless-it

Jemi dëshmitarë se përdorimi i rrjetit wireless (pa tela) është në rritje të shpejtë, ngase është i përshtatshëm për t'u përdorur. Megjithatë, rrjetet pa tel janë të prekshme prej hakerëve dhe vjedhjes së të dhënave, nëse nuk sigurohen. Prandaj duhet pasur kujdes gjithmonë për të mbajtur rrjetin pa tela në shtëpi të sigurt. Sigurimi i Wireless-it është përgjegjësi e të gjithë përdoruesve të kompjuterit. Nëse ju keni një rrjet pa tel në shtëpinë tuaj ju duhet të merrni hapat e mëposhtëm për të siguruar rrjetin tuaj pa tel.

Hapi 1

Ndrysho fjalëkalimin admin për të hyrë në router-in tuaj pa tel. Fjalëkalimet parazgjedhje në shumicën e wireless routers janë "admin", ose "password." Hakerët e dinë se këto fjalëkalime janë të paracaktuara për të hyrë në shumicën e routerëve dhe kjo është arsyeja pse ju duhet të ndryshoni fjalëkalimin.

Hapi 2

Ndrysho emrin e SSID (Service set identifier) e rrjetit tuaj pa tel dhe fik transmetimin. SSID është emri i rrjetit tuaj pa tel. Nëse transmetimi ne SSID tuaj e keni “on” të gjithë mund ta shohin emrin e rrjetit tuaj. Ju duhet fikur transmetimin kështu që askush tjetër nuk mund ta shohin emrin e rrjetit tuaj pa tel.

Hapi 3

Kriptoni Wireless-in tuaj me WEP ose WPA. Ju rekomandojmë të përdorni WPA me opsion AES. WPA do të kripton rrjetin tuaj pa tel dhe të kërkojë një fjalëkalim për të hyrë në të. AES ofron shifrim 28 bit dhe është përdorur nga qeveritë për të mbrojtur të dhënat. AES nuk është vetëm i sigurt, por është gjithashtu shumë i shpejtë. Fjalëkalimin që e keni krijuar për qasje në rrjetin juaj duhet të jetë kompleks dhe mbi 10 karaktere.

Rrjetet Wireless publike

Janë rrjetet wireless free që i përdorim në vende publike si kafene, qendra tregtare, etj. Këto rrjete wireless janë plotësisht të hapura për publikun dhe nuk kanë asnjë siguri.