



Shfletimi i sigurt i Internetit

Editor

Materiali është marrë nga trajnimet The SANS Institute (the Escal Institute of Advanced Technologies), dhe është kthyer në buletin (Newsletter) nga Sektori i Mbrojtjes Kibernetike, në kuadër të Departamentit për Komunikim dhe Teknologji Informative.

Ju lutem nëse keni ndonjë paqartësi, mos hezitoni të na kontaktoni.

Problemi

Interneti është bërë një nga mjetet tuaja më të fuqishme për shumë detyra, të tilla si kërkimi i informacionit, komunikimi me miqtë dhe bashkëpunëtorët, blerja në internet dhe menaxhimi i financave tuaja. Pothuajse në të gjitha këto raste mjeti kryesor që përdorni është shfletuesi juaj, siç janë Internet Explorer, Chrome ose Mozilla Firefox. Shfletuesi juaj është në shumë mënyra porta juaj drejt internetit.

Për shkak se kaq shumë njerëz në mbarë botën përdorin dhe varen nga shfletuesit për aktivitetet e tyre të përditshme në internet, shfletuesi juaj është gjithashtu një objektiv kryesor për kriminelët në internet. Kriminelët kibernetikë në të gjithë botën kanë zhvilluar sulme të reja dhe kanë krijuar faqe interneti me qëllim të keq, të dizajnuara për të hakuar shfletuesin tuaj dhe infektuar kompjuterin tuaj.

Sapo të hakohen, sulmuesit shpejt fitojnë kontrollin e plotë të kompjuterit tuaj dhe të gjithë informacionit tuaj pa e ditur ju atë. Duke mbrojtur shfletuesin tuaj dhe duke e përdorur atë me mençuri, ju mund të mbroheni kundër këtyre kërcënimeve dhe të përdorni me siguri internetin për aktivitetet tuaja të përditshme.

Mbrojtja e shfletuesit tuaj

Shfletuesi juaj i uebit është mjeti juaj kryesor për përdorimin e internetit. Ai është gjithashtu objektivi numër një për kriminelët në internet. Duke mbrojtur shfletuesin tuaj, ju mbron veten kundër shumë prej sulmeve të sotme.

Shmangia e lagjeve të këqija

Në shumë mënyra, Interneti është si një qytet i madh. Ka gjithçka që ju nevojitet, nga bankat dhe qendrat tregtare deri tek ngjarjet sportive dhe filmat. Sidoqoftë, ashtu si çdo qytet i madh, Interneti ka lagje të mira dhe lagje të këqija. Lagjet e mira përbëhen nga faqe interneti miqësore që i njihni dhe i vizitoni. Këto janë faqe në internet që zakonisht nuk do të përpiqen t'ju dëmtojnë.

Fatkeqësisht, ashtu si në shumicën e qyteteve të mëdha ka edhe lagje të këqija në internet. Këto lagje janë pjesë e internetit ku faqet e internetit janë krijuar për të sulmuar ose dëmtuar ju ose kompjuterin tuaj. Disa nga këto faqe interneti shpërndajnë softuer të infektuar, mbrojtës të tillë të rremë të ekranit ose lojëra të infektuara që do të pushtojnë kompjuterin tuaj.



Këtu janë hapat që mund të ndërmerrni për të mbrojtur shfletuesin tuaj dhe veten.

Zgjidhja

1. Shfletuesi juaj. Një hap kryesor për të mbrojtur shfletuesin tuaj është kur është e mundur, përdorni versionin më të fundit. Kompania që ka zhvilluar shfletuesin tuaj është duke shtuar vazhdimisht masa dhe veçori të reja të sigurisë për të rritur mbrojtjen e saj. Duke përdorur versionin e fundit ju siguroheni që keni mekanizmat më të fundit të sigurisë në vend.

Përveç funksionimit të versionit më të fundit, sigurohuni që shfletuesi juaj të jetë gjithmonë i përditësuar.

Kriminelët në internet po gjejnë vazhdimisht dobësi të reja në programin e shfletuesit. Si rezultat, shitësi i shfletuesit tuaj po lëshon vazhdimisht arna (patches) të reja për të rregulluar këto dobësi të njohura. Për të siguruar që shfletuesi juaj është gjithmonë aktual, aktivizoni përditësimin automatik.

Me përditësimin automatik të shfletuesit tuaj kontrolloni vazhdimisht për të parë nëse ka ndonjë arna të re, sapo të lëshohet një azhurim(update) i ri shfletuesi juaj ose sistemi operativ do të shkarkojë këtë azhurim dhe do të përditësojë shfletuesin.

2.Shmangni Shtojcat (Plugins)

Shtojcat ose Shtesa(Add-ons) janë programe shtesë që mund t'i instaloni në shfletuesin tuaj për t'ju dhënë më shumë funksionalitet. Për shembull, Adobe Flash, Java ose Apple QuickTime. Çdo shtojcë që shtoni bëhet një dritare tjetër për sulmuesit që të depërtojnë në kompjuterin tuaj. Për më tepër, mund të jetë e vështirë t'i mbash aktuale këto shtojca sepse shumë pak prej tyre kanë veçori të azhurnimit automatik. Instaloni vetëm shtojcat që janë të autorizuar dhe që ju nevojiten absolutisht, dhe sigurohuni që gjithmonë të keni të instaluar versionin e fundit.

3. Skanoni të gjitha shkarkimet. Për më tepër, një hap kryesor për të mbrojtur veten është skanimi i të gjithë dokumenteve të shkarkuar nga Interneti me antivirus të azhurnuar. Kur shkarkoni dhe instaloni ose ekzekutoni një program të ri, ai program mund të jetë i infektuar. Mund të duket se funksionon mirë, por në fakt ai do të përpiqet të infektojë në heshtje kompjuterin tuaj. Kjo është shumë e zakonshme veçanërisht me programet falas, siç janë ruajtësit e ekraneve ose lojërat falas.

Uebfaqe të tjera me qëllim të keq do të përpiqen të sulmojnë dhe hakojnë kompjuterin tuaj kur ju thjesht lidheni me to. Ashtu si në një qytet të madh, një nga mënyrat më të thjeshta për të qëndruar të sigurt është shmangia e lagjeve të këqija.

Nëse nuk keni dëgjuar kurrë për uebfaqen më parë, nëse informacioni i URL -së duket i pasaktë ose i dyshimtë, ose nëse faqja e internetit duket se ka informacion të dyshimtë, atëherë mos shkarkoni asnjë softuer dhe as mos i dorëzoni ndonjë informacion atij. Ndonjëherë është e vështirë të thuhet nëse një faqe në internet është e mirë apo e keqe, kjo është arsyeja pse është gjithashtu e rëndësishme të merren të gjitha masat paraprake të tjera të përshkruara në këtë gazetë.



Sigurohuni që të skanoni gjithçka që shkarkoni me antivirus para se ta hapni ose ta përdorni

4. Filtrimi dhe mbrojtja e faqeve të internetit. Filtrimi i faqes në internet të shfletuesit (i quajtur shpesh Filtrimi i ekranit të mençur, lista e zezë ose mbrojtja nga phishing) do t'ju ndalojë të vizitoni uebfaqe të rrezikshme që mund të përpiqen të sulmojnë shfletuesin tuaj dhe ju. Ju mund të mos e kuptoni, por ka faqe në internet që janë krijuar për të goditur shfletuesin ose kompjuterin tuaj vetëm duke i vizituar ato. Filtrimi i faqeve në internet është një listë e këtyre faqeve të njohura, të rrezikshme që nuk dëshironi t'i vizitoni. Ka me mijëra faqe të tilla në internet sot. Nëse përpiqeni të vizitoni njërin nga këto uebfaqe të njohura, me qëllim të keq, filtrimi i faqes në internet do të bllokojë përpyekjen tuaj dhe do t'ju shpjegojë se po përpiqeni të vizitoni një faqe (site) të njohur, me qëllim të keq. Shumica e shfletuesve të internetit e kanë aktivizuar këtë veçori si parazgjedhje, megjithatë ju duhet të kontrolloni dy herë për të qenë të sigurtë që i juaji është gjithashtu i aktivizuar.

5. Cilësimet shtesë të sigurtisë. Përveç asaj që kemi diskutuar deri më tani, një hap tjetër që mund të bëni është ndryshimi i cilësimeve të sigurtisë në shfletuesin tuaj. Disa shfletues të tillë si Internet Explorer kanë cilësime shtesë të sigurtisë së shfletuesit. Ju mund të dëshironi të merrni parasysh konfigurimin e cilësimeve tuaja të sigurtisë në një nivel më të lartë. Ndërsa mund të ndalojë funksionimin e disa faqeve legjitime, do të ecë përpara në mbajtjen e sistemit tuaj të sigurt.

6. Pajisjet celulare. Mbani në mend se këto udhëzime nuk janë vetëm për kompjuterin tuaj, por për çdo pajisje të mençur që mund të përdorni, përfshirë smartfonët ose tabletët. Ndërsa shfletuesit në pajisjet celulare mund të kenë më pak veçori dhe më pak opsione, ju prapë duhet ta mbani të sigurt. Siç diskutuam në faqen e parë, një nga gjërat më të rëndësishme që mund të bëni për ta mbajtur shfletuesin tuaj të sigurt në pajisjet celulare është të ekzekutoni gjithmonë versionin e fundit.