Tölvan III

Veiruvarnir og öryggi

STARFSGREINAFÉLAG

Til góðra verka!

Tölvuveirur (vírusar) eru til fyrir öll stýrikerfi en langflestar eru fyrir Microsoft Windows því það er langalgengasta stýrikerfið og þar með stærsta „skotmarkið". Tölvuveirur eru af ýmsum gerðum og verður þeim helstu lýst hér. Nýrri veirur eru þó oft samsettar og hafa eiginleika margra þessara flokka.

- **Veirur** eru forrit sem koma sér fyrir innan í öðrum forritum, til dæmis með því að bæta kóða sínum aftan við upphaflega forritið. Veiran breytir forritinu þannig að hún fær alltaf stjórnina um leið og það er ræst. Þetta gerir henni kleift að smita fleiri forrit sem hún finnur og skemma jafnvel gögn. Veirur dreifast handvirkt þegar smituð forrit eru flutt yfir á aðra ósmitaða tölvu.
- **Macro-veirur** smita skjöl frá forritunum í Microsoft Office, til dæmis Word- og Excel-skjöl. Fjölvamálið (macro) í Microsoft Office er mjög öflugt og því er hægt að misnota það til að skrifa veirur sem dreifa sér í skjölum. Einnig er hægt að skrifa með því Macro-orma sem senda sjálfa sig sjálfkrafa með tölvupósti.
- **Ormar** eru sjálfstæð forrit sem sjá um sína eigin dreifingu. Helstu tegundir eru **póstormar** sem dreifa sér sjálfir í tölvupósti og **netormar** sem dreifa sér beint á milli nettengdra tölva. Netormar nýta sér veikleika eða galla í stýrikerfum til að dreifa sér sjálfvirkt en póstormar reyna oftast að gabba viðtakandann til að opna viðhengi sem fylgja tölvupóstinum.
- **Spam-ormar** eru forrit sem dreift er í miklu magni með tölvupósti á sama hátt og ruslpósti. **Þjarkar** *(e.Bots)* eru forrit sem stjórnað er í gegnum bakdyr og senda t.d. út ruslpóst, án samþykkis eiganda tölvunnar. Spam-ormar geta ekki dreift sér sjálfir heldur er þeim dreift af illkvittnum aðilum sem viðhalda **þjarkanetum**. Allur tími sem ekki fer í ruslpóstsendingar er nýttur til að senda út nýjar útgáfur af ormum og þjörkum sem smita fleiri tölvur og stækka þannig og viðhalda dreifingarnetinu.
- **Bakdyr** (*e. Backdoors)* eru forrit sem opna aðgang að tölvunni fyrir utanaðkomandi aðilum – án samþykkis eiganda. Slíkur aðgangur leyfir tölvuþrjótum að nota tölvuna eins þeim þóknast.
- **Njósnahugbúnaður** *(e. Spyware)* fylgist með allri notkun á tölvunni og sendir upplýsingar um þá notkun til utanaðkomandi aðila án samþykkis eiganda tölvunnar. Slíkur hugbúnaður er helst notaður til að stela greiðslukortaupplýsingum og aðgangsupplýsingum (notandanöfnum og lykilorðum).
- **Trójuhestar** eru forrit sem villa á sér heimildir og gera annað en notandinn býst við að þau geri. Dæmi um trójuhest er tölvupóstur sem reynir að fá notandann til að opna viðhengi sem inniheldur tölvuveiru með því að segja að viðhengið sé skemmtilegur leikur eða það geymi mikilvægar upplýsingar.

Veiruvarnir eru nauðsynlegar öllum tölvum sem tengdar eru Internetinu. Þaðan berast flestar veirur í tölvur, bæði beint gegnum netið og líka með póst og samskiptaforritum. Veiruvarnarforritin **Avast!** og **AVG** er hægt að sækja á netið án endurgjalds og nota á einkatölvum. Ekki er leyfilegt að nota þennan hugbúnað á atvinnutölvum.

Til eru mörg veiruvarnarforrit. Þekktust þeirra eru Norton Antivírus, F-Prot og Trend. Þau er hægt að kaupa í tölvuverslunum og á netinu. Á netinu er líka boðið upp á að leita tölvuna þína yfir netið. Slóðin er *housecall.trendmicro.com*. Þar smellirðu á **„Scan now, It's free"** og samþykkir skilmálana.

AVAST! - Slóðin er *www.avast.com*.
Veldu Download – Programs – **Avast 4 Home Edition FREE Download.** Þar geturðu sótt forritið, en einnig er þar tengill á skráningarsíðu, þar sem þú þarft að skrá þig og gefa upp netfang. Á slóðinni www.avast.is er að finna upplýsingar um forritið á íslensku. Vistaðu skrána á vísum stað, finndu hana aftur og tvísmelltu á hana þegar niðurhali er lokið. Þá fer í gang uppsetningarferli, þar sem þarf að smella nokkrum sinnum á **NEXT** og haka við **I agree**. Að lokum er smellt á **Finish** og þá kemur upp gluggi sem býður upp á skönnun eftir endurræsingu. Ef engin vörn var á vélinni fyrir eða grunur er um smit, er best að smella á Yes og endurræsa tölvuna. Skannið sem þá fer í gang getur tekið töluverða stund.

Þegar það skann er búið, þarf að opna forritið með því að smella á bláa A-hnöttinn neðst í hægra horninu.
Þá sækir forritið nýjustu veiruupplýsingarnar og er tilbúið til notkunar.

Avast! virkar í 60 daga án skráningar en lykillinn sem þú færð sendan ef þú skráir þig, gildir í eitt ár. Hann kostar þig ekkert annað fyrirhöfnina við að sækja hann.

AVG - Slóðin er *free.avg.com*.

Veldu **Download – AVG Anti-Virus Free Edition 8.0.** Þar er tengill til að ná í forritið. Vistaðu skrána á vísum stað og tvísmelltu á hana þegar niðurhali er lokið. Þá fer í gang uppsetning þar sem þarf að samþykkja og ýta á OK af og til. Að uppsetningu lokinni keyrir forritið **First run Wizard,** þar sem ýmsir valkostir eru í boði. Þar er boðið upp á uppfærslu (**Update**) og er nauðsynlegt að velja hana ef verið er að setja forritið upp í fyrsta skipti. Loks er boðið upp á skráningu, en hún er valfrjáls og hefur ekki áhrif á vinnslu forritsins. Að loknu þessu ferli, geturðu smellt á merki AVG hvort sem er á skjáborðinu eða neðst í hægra horninu og séð hvort varnirnar þínar eru í lagi.

Fleiri veiruvarnarforrit

Ýmsar aðrar varnir eru fáanlegar á netinu án endurgjalds en ekki verður farið í nánari lýsingu á uppsetningu þeirra. Þó er rétt að nefna forrit sem koma í veg fyrir og hreinsa burt óumbeðnar auglýsingar og annað slíkt sem óhjákvæmilega fylgir netnotkun. Þar eru forrit eins og **Ad-Aware** frá Lavasoft *(www.lavasoft.com)*, sem upphaflega voru hönnuð í þessum tilgangi, en hafa síðan þróast yfir í veiruvarnarforrit. Ad-Aware er hægt að fá ókeypis til heimilisnota eins og þau tvö sem áður voru nefnd.

„Einhver braust inn í tölvuna þína, en það virðist ekki hafa verið reyndur tölvuþrjótur."

Spybot – Search & Destroy er eingöngu hannað í þeim tilgangi að hreinsa burtu njósnaforrit og auglýsingar, en er ekki veiruvarnarforrit sem slíkt. Það er að finna á slóðinni *www.safer-networking.org*

Nokkrar góðar reglur:

- Opnaðu aldrei póst sem þér finnst einkennilegur, hentu honum strax!
- Opnaðu ekki viðhengi með pósti nema þú vitir hvað það er. Þó þú þekkir sendandann getur tölvan hans verið sýkt af veiru.
- Hafðu alltaf virkt veiruvarnarforrit í tölvunni þinni og uppfærðu það reglulega. Best er að hafa uppfærsluna sjálfvirka.
- Uppfærðu stýrikerfi tölvunnar þinnar reglulega. Best er að nota sjálfvirkar uppfærslur (Automatic updates) sem sækja allar mikilvægar uppfærslur sjálfkrafa og láta þig vita að þær þurfi að keyra inn.
- Samþykktu aldrei óumbeðna innsetningu forrita.

Tölva án veiruvarna er eins og ólæst hús. Þangað komast allir inn og geta gert það sem þeim sýnist.

Aðrir bæklingar í þessari ritröð:

- **Tölvan I** - *Stýrikerfið Windows XP*
- **Tölvan II** - *Jaðartæki*

STARFSGREINAFÉLAG

Til góðra verka!