Pred vama se nalazi drugo izdanje "Priručnika za računalnu sigurnost korisnika Interneta". Ovaj Priručnik rezultat je više nego dobrih reakcija na prvo izdanje kao i želje da i dalje korisnicima Interneta pomognemo savjetima iz područja računalne sigurnosti.

Popularno je nazvan "Borbeni komplet" jer se uz Priručnik u kojem su na jednostavan i razumljiv način obrađene aktualne teme iz područja računalne sigurnosti nalazi i CD na kojem su besplatni alati koji pomažu korisniku da podigne razinu sigurnosti svojeg računala.

Priručnik je namijenjen korisnicima operacijskog sustava Microsoft Windows, no sadrži i neke općenite savjete koji vrijede za sve operacijske sustave.

Pozivamo vas da pažljivo proučite Priručnik u kojem su opisani teoretski i praktični aspekti osnova računalne sigurnosti i naučeno primijenite u praksi, čime povećavate razinu sigurnosti cjelokupnog Interneta.

Nadamo se da ćemo vam ovim Priručnikom pomoći adekvatno zaštititi vaše računalo kako bi mogli nesmetano koristiti sve prednosti Interneta.

Sigurno korištenje Interneta želi vam
CARNet CERT tim

SADRŽAJ

05 **Upoznajmo neprijatelja**

05 **Svijet u velikom**

05 Buntovnici bez razloga

05 Razlozi bez buntovništva

06 **Svi putovi vode - svugdje**

06 Dosegnuti mrežu

07 Zona slobodnog leta

08 **Oni su među nama**

08 Ali to nije sve

09 Tajna šaputanja

11 **Snage sigurnosti**

11 **Obrana na vlastitom teritoriju**

11 Napad ispod radara

12 Specijalne jedinice

13 **Granična kontrola**

13 Međuračunalni dolasci

14 Međuračunalni odlasci

16 **Uvijek spremni**

16 Potrebe se razlikuju

17 Gerilsko surfanje

18 **Pričuvna država**

18 Što sve čuvamo

19 Strategije

20 **Obavještajni incidenti**

20 **Ne vjeruj Danajcima ni kad darove nose**

21 Bodljikava pošta

21 Odluka je vaša
22 **Je li vuk pojeo banku?**
23 Ne, ja sam Pero Korisnik
24 Čuvajte svoje ja
25 Prepoznajte svoje ja
26 **Izgleda li kao prijevara i miriše na prijevaru**
27 Vrlo stvarna opasnost

30 **Priprema bojišta**
30 **Uspostavljanje prve linije**
31 Ugradnja ZoneAlarm vatrozida
32 **Odabir diplomata**
34 Nakon ugradnje Mozilla Firefox web preglednika
35 Alternativa za elektroničku poštu
36 **Razmještanje trupa**
36 Ugradnja i podešavanje avast! antivirusnog alata
36 Nakon ugradnje
38 Anti-spyware
40 **Održavanje pripravnosti**
41 Kontrolna soba
42 Windows Security Center
43 Ažuriranje preporučenih programa
44 **Civili na sigurnom**
44 Izrada sigurnosne kopije operativnog sustava
45 Arhivske kopije multimedije
46 Iz dana u dan

50 **Pojmovnik**

U malim, sigurnim sredinama ne zaključavaju se vrata. Svi se međusobno poznaju i krivcu bi se bilo teško sakriti. Internet je također nekada bio mala sredina. Na njemu jednostavno nije bilo mnogo sadržaja koji bi zanimali vanjski svijet. Akademski korisnici, koji su Internet stvorili i u to se vrijeme jedini njime služili imali su zajednički interes. Računalnog kriminaliteta nije bilo pa nije bilo ni potrebe da se od njega na bilo koji način štiti.

Danas je Internet napučen poput najmnogoljudnijih zemalja svijeta. Broji oko milijardu korisnika[1] koji se na mrežu spajaju iz svih krajeva svijeta. Ima vlastitu infrastrukturu, nadležne službe, mogućnosti koje nudi pa čak i svoju specifičnu kulturu. Na žalost, kao i pravi velegrad, Internet vrvi najrazličitijim oblicima kriminala.

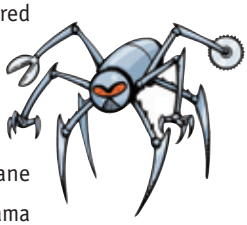
Naučili ste zaključavati vrata svojega stana i ne ostavljati dragocjenosti na vidljivom mjestu bez nadzora. Jednako tako možete naučiti i kako sigurno koristiti Internet.

[1]podatak preuzet s http://www.internetworldstats.com

UPOZNAJMO NEPRIJATELJA

SVIJET U VELIKOM

Gotovo sve što biste očekivali pronaći u zemlji s milijardu stanovnika pronaći ćete i na Internetu. Tu su trgovine, turističke agencije, banke, knjižnice, čitav jedan svijet usluga zajedno s njihovim uređenjem i službama koje ga provode. Svaki uređen svijet narušen je onima u njemu koji taj red ne poštuju, jer ljudi uvijek nalaze načine da prevare sustav.



Buntovnici bez razloga

U vrijeme dok se na Internetu uglavnom nisu odvijale novčane transakcije, pisanje samoumnažajućih (*virusi, crvi*) ili zlonamjernih programa (*malware*) bilo je namijenjeno izazivanju pažnje - nije bilo moguće na taj način ostvariti materijalnu dobit. Danas su ovakvi primjeri rijetkost, a *malware* se sve češće koristi u kriminalne svrhe.

Vandalizam nije nestao razvojem računalnog kriminala. Nalazimo ga u obliku sličnom uništavanju javnih površina grafitima - ***web defacementu***, odnosno neovlaštenom mijenjanju sadržaja tuđih web stranica.

Razlozi bez buntovništva

Lanci sreće blaži su oblici **prijevare** u kojoj stradava naše vrijeme, ali i privatnost tuđih adresa elektroničke pošte. Jednako kao što vi na takvoj poruci vidite sve kojima je ona poslana, vide i oni koji su ih spremni iskoristiti za slanje neželjene pošte (*spama*). Mnogo su opasnije lažne humanitarne akcije, igre na sreću, krediti ili pak nevjerojatne prilike brze zarade velikih količina novca. Iza njih se često kriju beskrupulozni kriminalci, bez obzira jeste li njihovu ponudu našli pod brisačem ili u pretincu elektroničke pošte. U tom se pretincu u današnje vrijeme nalazi

velika količina neželjene pošte, ***spama***. Kada ga otvarate, u njemu će vjerojatno biti više šarenih kataloga nego vaše željene pošte. Za razliku od vašeg fizičkog sandučića, u koji stižu samo reklame vezane uz vaš grad i bližu okolicu, u pretinac elektroničke pošte stižu reklame (i prijevare) iz čitavog svijeta. Na Internetu je svejedno u kojem se dijelu svijeta nalazite.

Kriminalci će se na razne načine pokušati domoći vaših pristupnih podataka (podataka koje unosite da biste pristupili usluzi). Te podatke iskoristit će da bi se predstavili kao vi i koristili usluge u vaše ime. Najčešći način na koji dolaze do vaših podataka odvija se putem poruka elektroničke pošte u kojima se od vas traži da na nekoj web stranici upišete svoj PIN, zaporku ili neki drugi povjerljiv podatak. Poruka, naravno, izgleda kao da je poslana od vašeg davatelja usluge.

SVI PUTOVI VODE - SVUGDJE

Osnovna je karakteristika Interneta međusobna povezanost svih računala. Za spajanje na Internet potrebno je spojiti se na računalo već uključeno u mrežu.

Dosegnuti mrežu

Uslugu spajanja s računalom već povezanim na Internet omogućava vam ISP (Internet Service Provider, pružatelj usluge Interneta). Njegova je uloga premostiti "*posljednju milju*" do korisnika.

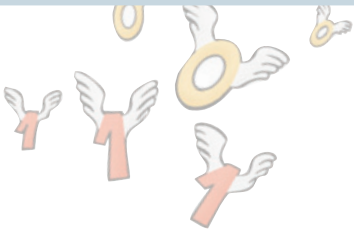
Dial-up, odnosno pristup putem telefonskog poziva danas je još uvijek dominantan pristup Internetu u Hrvatskoj. Vaše računalo putem telefona *razgovara* s računalom ISP-a i na taj način ostvaruje povezanost, što znači da je veza ostvarena samo za trajanja telefonskog poziva. Budući da su klasični telefonski pozivi ipak prvenstveno namjenjeni govornoj komunikaciji, računala na ovaj način ostvaruju relativno niske brzine prijenosa podataka.

DSL i ***kablovske veze*** koje ubrzano zamjenjuju dial-up omogućavaju veće brzine prijenosa podataka. Zbog modela naplate kojim se ne mjeri vrijeme provedeno na Internetu, mnogi korisnici vezu s Internetom ne prekidaju kada im više nije potrebna, već samo kada isključe računalo.

Bežične veze također su tipično stalne (ne uključuju se po potrebi već su čitavo vrijeme aktivne). Pružatelj usluge u pravilu vodi brigu o njihovoj sigurnosti pa se na njih ne odnose iste opasnosti kao na **bežične lokalne mreže**.

Zona slobodnog leta

Bežične lokalne mreže (WLAN, najčešće isporučene u sklopu ADSL usluge) po svojoj su prirodi izloženije neovlaštenom spajanju. S obzirom da nije potrebno imati fizički pristup nekom priključnom mjestu, one su dostupne svakome tko se nalazi u dometu (npr. vašim susjedima). Zbog toga je pristup takvim mrežama potrebno dodatno osigurati, ako vaš pružatelj usluga to već nije učinio pri ugradnji.



Nezaštićene bežične mreže čine vaše zaporke i druge povjerljive podatke koji putuju mrežom čitljivima svakome tko se nalazi u dometu. Imate li putem takve mreže omogućen i pristup Internetu, vaši susjedi se na vaš račun njime mogu koristiti.

ONI SU MEĐU NAMA

Šarolikost među programima koji čine štetu dovela je do zbrke u nazivima koji se za njih koriste. Virusi, za koje najčešće čujemo, danas su najrjeđi pojavni oblik **nametnika**. Na engleskom jeziku susrećemo naziv ***malware***, što znači zlonamjeran program.

Crvi i virusi često usporavaju računalo do neupotrebljivosti i ponekad prisiljavaju naš ISP da nam uskrati uslugu da bi zaštitio ostale korisnike. Naime, naše se računalo, jednom zaraženo, potajno koristi za distribuciju ilegalnog sadržaja i *spam* poruka te koordinirane napade na druga računala.

Ali to nije sve

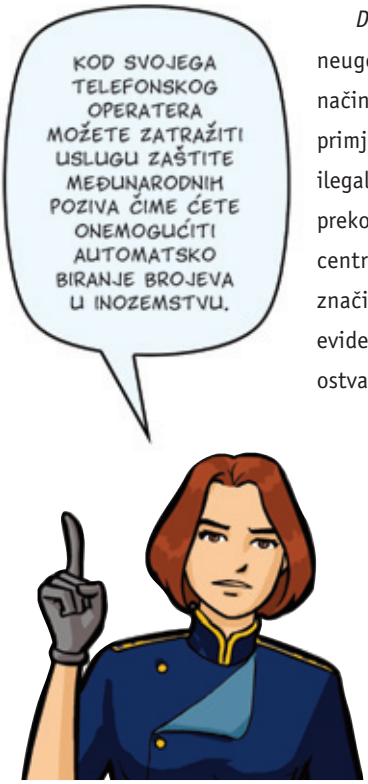
Milijardu korisnika svakog će trgovca zainteresirati kao potencijalno tržište. Oni među njima koji nisu spremni financirati legalnu kampanju i pristup dobrovoljnim potrošačima služe se krajnje nasilnim metodama da bi saznali što najčešće kupujemo i zatim nas zasuli s ponudama. **Spyware** nas uhodi i bilježi stranice koje posjećujemo, a **adware** nas obično bez pitanja zatrpava reklamnim porukama. Poznati su vam iskačući, ***pop-up*** prozori puni reklama? Upravo njih pokreće adware.

Spyware i adware vezani su uz web, kojeg najviše koristimo za svoje dnevne potrebe. Do nas se probijaju zlouporabom nesavršenosti našeg web preglednika ili nagovaranjem nas, korisnika, da preskočimo sigurnosna upozorenja. Jednom kada se domognu kontrole nad našim računalom, vrlo će se efikasno *ugnijezditi* i nastojati što bolje iskoristiti kratko vrijeme koliko predviđaju da ćemo im tolerirati ostanak. Stoga takvi programi obično u kratkom roku učine računalo potpuno neupotrebljivim i jedino što pomaže je ponovna ugradnja i postavljanje operativnog sustava.

Tajna šaputanja

Da bi pojednostavnili plaćanje svojih usluga, mnogi servisi kojima pristupate telefonom naplaćuju svoju uslugu u sklopu cijene telefonskog poziva (primjer su brojevi koji počinju s **060**). Tako telefonom možete sudjelovati u nagradnim igrama, dobivati informacije, koristiti komercijalne službe za tehničku pomoć i slično.

Ovaj koncept proširen je i na korištenje komercijalnog sadržaja web stranica - da biste platili korištenje sadržaja, spajate se izravno na pružatelja sadržaja umjesto na Internet, a cijenu razgovora plaćate po nekoj drugoj tarifi. Pri tome koristite ***dialere***, programe koji tu vezu ostvaruju.



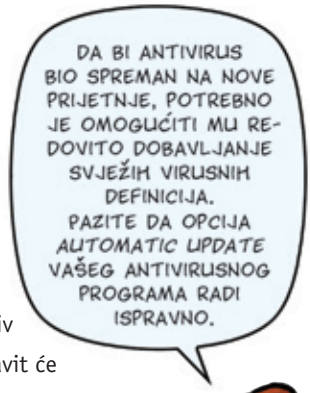
Dialeri se danas gotovo isključivo vežu uz neugodna iznenađenja na telefonskom računu. Ovaj način naplate u tolikoj se mjeri zloupotrebljava da su primjeri legalne upotrebe gotovo iščezli. Tipično, ilegalni *dialeri* ostvaruju astronomski skupe pozive u prekooceanske zemlje i to korištenjem telefonskih centrala u državama koje slabo provode zakone. To znači da svoj novac ne možete više vratiti, iako je evidentno da ste prevareni. Povrh toga, pozivi će biti ostvarivani i bez da vi to zatražite.

OBRANA NA VLASTITOM TERITORIJU

Virusi i crvi nametnici su kojima smo bombardirani čim se povežemo na Internet. Pokušavaju na naše računalo prodrijeti putem elektroničke pošte, P2P alata, *instant messaging* programa i mnogih drugih mogućnosti našeg računala kojih nismo ni svjesni. Pobrinimo se da ih dočeka ljut otpor. Od djelovanja samoumnažajućih programa (virusa i crva) borimo se prepoznavanjem i zaustavljanjem. **Antivirusni alati** za svaki pojedini virus ili crv imaju odgovarajuća "*antitijela*" koja zovemo **virusne definicije.**

Napad ispod radara

Metoda cijepljenja efikasna je protiv virusa i crva, jer ih njihova masovna rasprostranjenost dovodi i u laboratorije antivirusnih stručnjaka. Na žalost, na ovaj način obranili smo se samo od najočitijeg neprijatelja.



Trojanski konji se, kao u priči iz koje je naziv potekao, oslanjaju na naše povjerenje. Predstavit će nam se kao zanimljiv program, a možda i neki video ili audio sadržaj koji smo tražili. Svojevoljno ćemo mu dozvoliti izvršavanje na našem računalu. Ovakvi programi rijetko ili čak nikada ne dospiju u laboratorije antivirusnih stručnjaka, posljedica čega je da ih antivirusni alati ponekad ne uspiju prepoznati.

Specijalne jedinice

Spyware, adware i dialeri razvijaju se zapanjujućom brzinom, prevelikom da bi stručnjaci mogli s njima držati korak izrađujući virusne definicije. Često su kombinacija nametnika drugih oblika i istovremeno se služe brojnim metodama da bi se domogli kontrole nad našim računalom. Jednom kada se na njemu *nastane*, vrlo će dobro utvrditi svoje položaje.

Protiv ovih nametnika i trojanskih konja koji ih često prate borimo se **anti-spyware alatima**. Ovi alati u svojem osnovnom načinu rada prepoznaju nametnike koji se već nalaze na računalu i pokušavaju ih ukloniti. Također zahtijevaju redovito ažuriranje da bi mogli prepoznati nove prijetnje. Uklanjanje nametnika koji su već utvrdili položaje na vašem računalu nije nimalo lak zadatak i često jedan anti-spyware alat samostalno ne uspije obaviti sav posao. Zbog toga je poželjno koristiti dva ili više takvih alata.

Anti-spyware alati uglavnom pretražuju računalo na zahtjev[1], što znači da samom ugradnjom niste spriječili dolazak nametnika. Zbog toga je poželjno anti-spyware alate samostalno pokretati s vremena na vrijeme, a obvezno prije radnji koje uključuju trgovinu ili razmjenu povjerljivih podataka putem Interneta.

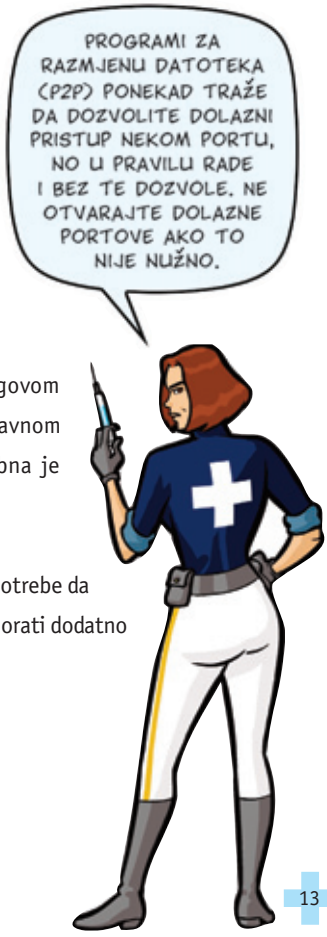
Postoje i komercijalna **integrirana rješenja** proizvođača sigurnosnih alata (antivirus, anti-spyware, vatrozid) koja vas aktivno brane od svih vrsta nametnika istovremeno, što predstavlja bolju, ali i skuplju kompletnu zaštitu.

[1]besplatni alati preporučeni u ovoj brošuri rade na ovaj način

GRANIČNA KONTROLA

Kolika god bila naša želja za sigurnošću, računalo ne možemo jednostavno izolirati od vanjskog svijeta. Redoviti prelasci *granice* koja nas dijeli od Interneta postupak su koji moramo dozvoliti, a kontrolu granice prepuštamo sigurnosnom alatu kojeg zovemo **vatrozid** (*firewall*). Naravno, ulazak i izlazak tretiraju se potpuno različito.

Pri ulasku u neku zemlju često vas dočeka pitanje o razlogu dolaska. Naš vatrozid također razlikuje posjetitelje po ovom kriteriju. Naime, većina komunikacije na Internetu započinje ostvarivanjem veze na neki ***komunikacijski port***. Riječ je o broju koji se dogovorno veže uz određeni tip usluge (npr. broj 80 označava uslugu *HTTP* i služi za web promet).



Međuračunalni dolasci

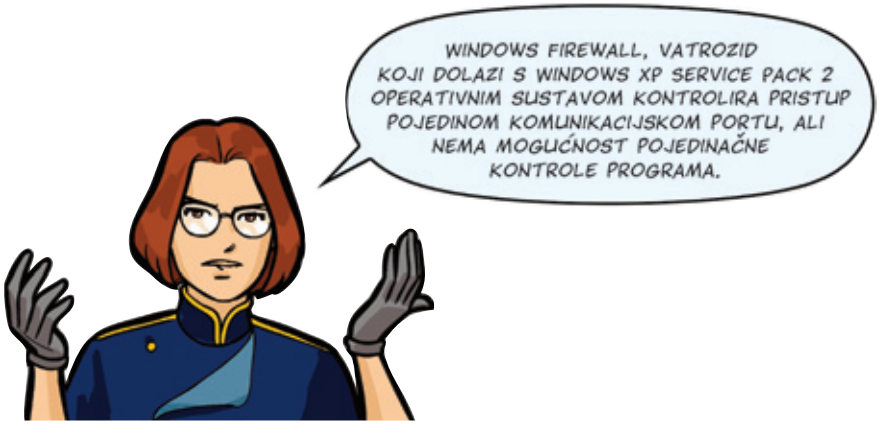
Tipičnom korisniku nije potrebna mogućnost da se njegovom računalu pristupa izvana, upravo zbog toga što on usluge uglavnom *koristi*, a ne *poslužuje*. Poslužiteljskim programima potrebna je mogućnost da im se pristupa s Interneta.

Gotovo svi korisnički programi mogu ispravno raditi bez potrebe da im se pristupa izvana, što znači da u tipičnom slučaju nećete morati dodatno podešavati vatrozid da propušta ulazak na nekim *portovima*.

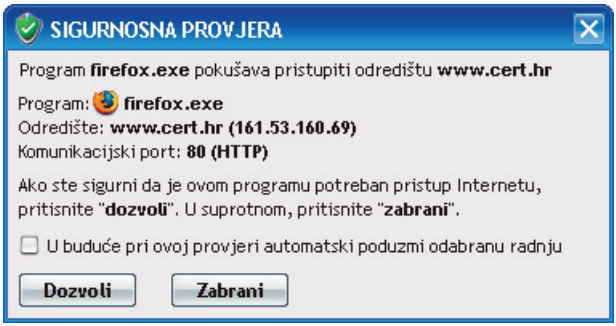
Međuračunalni odlasci

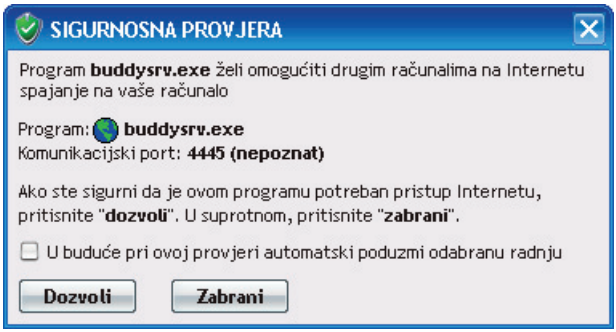
Kontrola odlazaka nešto je drugačija po svojoj prirodi, jer u tom nas slučaju više zanima *tko* odlazi nego *kamo* odlazi. Vatrozid[1] u ovom slučaju provjerava koji je program zahtijevao kakav pristup. Na taj način možemo ograničiti pristup Internetu na one programe kojima je taj pristup zaista potreban.

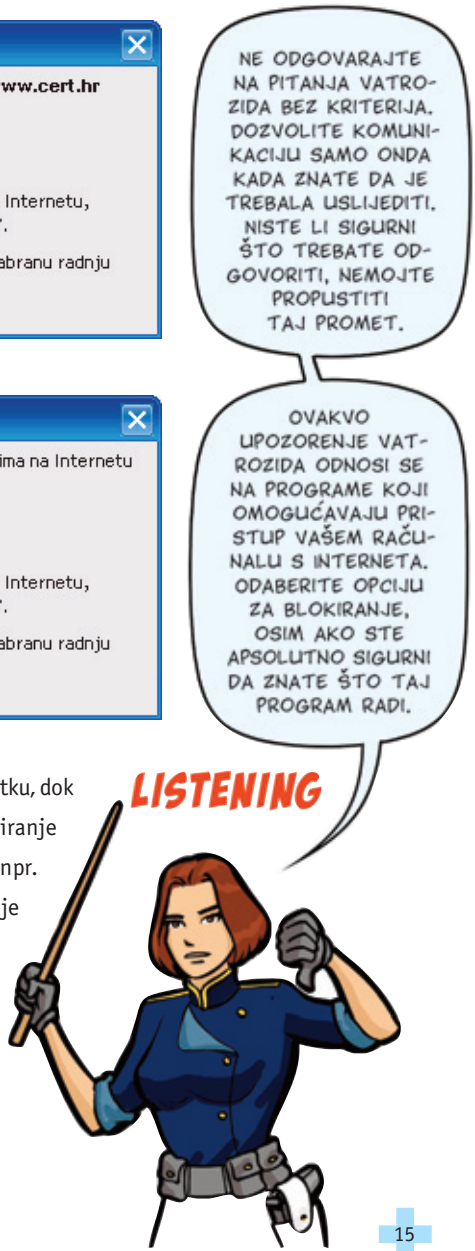
Vatrozidi ne dolaze s unaprijed postavljenim pravilima granične kontrole, već od korisnika očekuju da ih nauči što propustiti, a što ne. To učenje odvija se na način da vatrozid zaustavi program koji pokušava komunicirati s vanjskim svijetom, opiše taj pokušaj korisniku i pita ga za dopuštenje.



[1]vatrozid s opisanom mogućnošću zovemo aplikacijski vatrozid *(application firewall)*







Većina pitanja vatrozida pojavljivat će se u početku, dok ne "*nauči*" pravila koja ste mu postavili. Ažuriranje programa kojima je potreban pristup Internetu (npr. web preglednika) uzrokovat će ponovno postavljanje pitanja, jer vatrozid novu inačicu ne prepoznaje.

UVIJEK SPREMNI

Sigurnosni alati naše su trupe u borbi s prijetnjama Interneta. Bez njih bili bismo laka meta, no ipak nam osnovni cilj treba biti da do potrebe za njihovim djelovanjem ni ne dođe. Svaka dobro štićena organizacija u stalnom je stanju pripravnosti. Kontinuirano traži i ispravlja propuste u svojoj zaštiti i drži svoje snage u pripravnosti, obučene za borbu s aktualnim napadačima.

Potrebe se razlikuju

Osnovu svih programa na računalu čini operativni sustav, od kojih je na kućnim računalima najrašireniji Windows XP. Održavamo ga u pripravnosti

uz pomoć komponente ***Automatic Updates***, kojoj pristupamo kroz *Control Panel.*

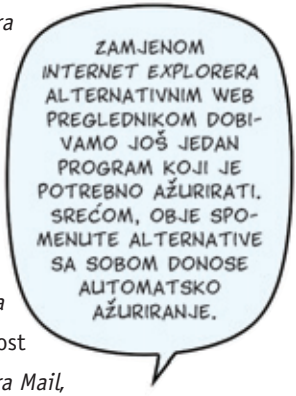
Svi sigurnosni alati moraju se redovito ažurirati da bi izvršavali svoju ulogu, no njihove pojedinačne potrebe su različite. Antivirusni alat ažurira se automatski, bez potrebe za našom intervencijom. Anti-spyware alate tipično ažuriramo neposredno prije upotrebe, a vatrozid nas povremeno obavijesti o dostupnosti novije inačice koju je potrebno ugraditi.

Ažuriranje je općenito važno za sve programe ugrađene u računalo. Zatraže li vas drugi programi i komponente na računalu dopuštenje za **ažuriranje (*update*)**, svakako im to dozvolite.

Gerilsko surfanje

Računalnim kriminalcima posao uvelike olakšava ujednačenost programa koje koristimo. Zamislite samo koliko bi kradljivcima automobila bilo lakše kada bi svi automobili imali jednake brave. Kako je naš najčešće korišten prozor u svijet naš web preglednik, upravo na njegove slabosti prijestupnici ciljaju ne bi li uz što manje truda stekli pristup što većem broju računala.

Internet Explorer, web preglednik ugrađen u *Windows* operativni sustav, najrašireniji je i najizloženiji izbor. Alternativu mu među ostalima predstavljaju *Mozilla Firefox* (http://www.getfirefox.com) i *Opera* (http://www.opera.com)[1]. Korištenjem **alternativnih programa** stavljamo se u grupu korisnika za kojima postoji manji interes kriminalne zajednice.

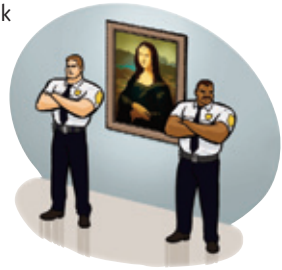


Alternativni programi postoje i za druge namjene: koristite li program za pregled elektroničke pošte, kao što je Outlook Express, znajte da i za njega postoje alternative. Već spomenuti *Mozilla Thunderbird* program je koji nudi sličan način rada uz manju izloženost tipičnim sigurnosnim prijetnjama, a slične prednosti donosi i *Opera Mail*, dostupna uz *Opera* web preglednik.

[1]web preglednici navedeni su redoslijedom procijenjene zastupljenosti na tržištu u vrijeme pisanja ove brošure, od najzastupljenijeg prema najmanje zastupljenom

PRIČUVNA DRŽAVA

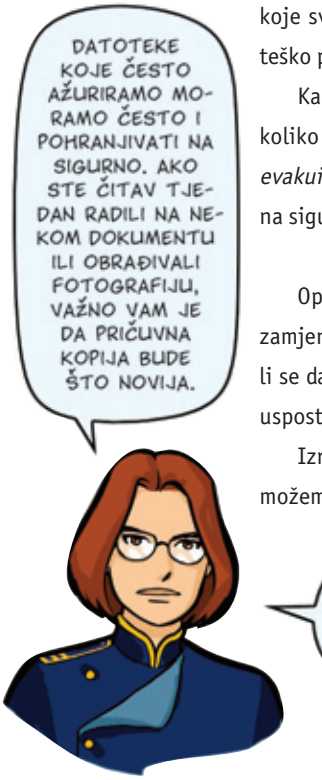
Ono najvrjednije što imamo u računalu najčešće nije ni brzi procesor ni najsuvremeniji optički pogon. Najvrjedniji su naši podaci koji mogu predstavljati naš višemjesečni rad i čiji bi gubitak bio veća šteta od gubitka čitavog računala. Na sreću, za razliku od računala, podatke možemo jednostavno umnažati i tako stvarati pričuvne kopije. Stvaranje pričuvnih kopija važnih podataka zovemo ***backup***.



Što sve čuvamo

Najveće dragocjenosti uglavnom ne zauzimaju velik prostor. Dokumenti koje svakodnevno unosimo i mijenjamo rijetko dosegnu veličinu koja se teško pohranjuje na neki prenosivi medij.

Kada govorimo o *backupu*, podatke prvenstveno razlikujemo po tome koliko ih često mijenjamo. **Često mijenjane podatke** moramo često *evakuirati*, dok je **stalne podatke**, kao što su fotografije, dovoljno pohraniti na sigurno neposredno nakon što su nastali.



Operativni sustav (*Windows*) i programi koje na njega ugrađujemo zamjenjivi su čuvamo li njihove medije ili datoteke u kojima dolaze. Dogodi li se da izgubimo samo njih, najveća je žrtva vrijeme potrebno za ponovno uspostavljanje radne okoline.

Izrazito **velike i lako povratne podatke**, kao što su računalne igre, možemo jednostavno izostaviti kada razmišljamo o *backupu*.

Strategije

Da bi *backup* bio što jednostavniji, važno je držati podatke odvojene po kriteriju promjenjivosti i veličine, po ranije opisanim kriterijima. To znači da ne miješamo dokumente s glazbom ili sistemske datoteke s fotografijama. Cilj nam je postići da u svakom trenutku pri ruci imamo:

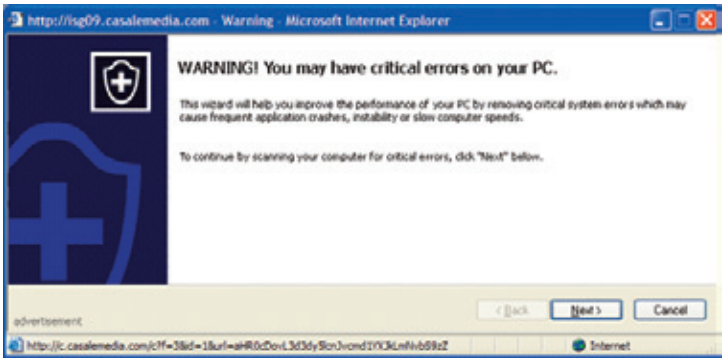
- krizni štab - kopiju stanja operativnog sustava neposredno nakon ugradnje i postavljanja
- arhivu - pričuvnu kopiju važne multimedije i drugog nepromjenjivog sadržaja
- posljednje položaje - nedavnu kopiju stanja svakodnevno ažuriranih dokumenata

OBAVJEŠTAJNI INCIDENTI

NE VJERUJ DANAJCIMA NI KAD DAROVE NOSE

Ni najbolja brava ne može nas zaštititi ako kriminalcima svojom voljom otvorimo vrata. Upravo zato se mnogi prevaranti oslanjaju na naše povjerenje kako bi izbjegli zamornu utrku sa sigurnosnim alatima.

Svakodnevno nam u pretinac elektroničke pošte stižu brojne poruke sumnjivog porijekla i sadržaja. Nismo li zatražili da nam ih se šalje, zovemo ih ***spam*** ili neželjena pošta. Među naizgled bezopasnim reklamama koje samo oduzimaju naše vrijeme i prostor, nalaze se i brojne prijevare, crvi i trojanski konji.



Neki oglašivači oponašaju izgled programa i njihovih upozorenja kako bi vas privukli na njihove stranice. U ovakvom slučaju, kliknite na tipku za zatvaranje prozora (crveni X). Klik na bilo koji drugi dio prozora poveznica je na stranice autora ove prevare.

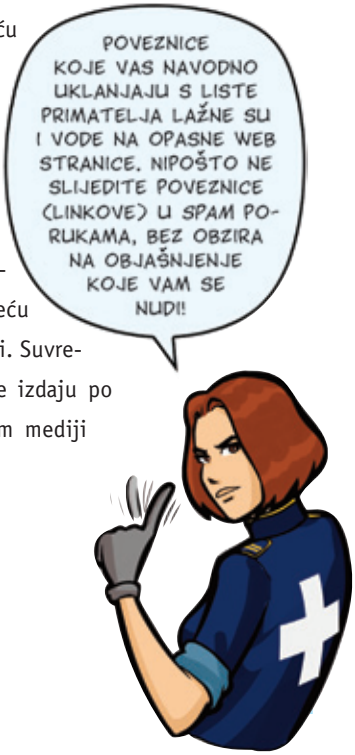
Bodljikava pošta

Opasne poruke nisu uvijek očite. Njih kreiraju majstori **socijalnog inženjeringa** - manipuliranja korisnicima u svrhu zaobilaženja sigurnosnih mehanizama. Primite li neobično primamljivu ponudu putem elektroničke pošte, potencijalna ste žrtva.

Vjerojatno ste već čuli kako privitke (***attachment***) iz nepoznatih izvora nipošto ne treba otvarati. To upozorenje odnosi se i na poznate izvore, niste li apsolutno sigurni da taj privitak očekujete. Prevaranti se gotovo uvijek lažno predstavljaju. Poznati slučajevi crva dolazili su predstavljajući se kao sigurnosne zakrpe od Microsofta.

Odluka je vaša

Napredovanjem sigurnosnih alata kriminalci se sve više okreću postavljanju poveznica (link) u svoje poruke. Te poveznice korisnike vode na još opasnije web stranice prepune svih oblika nametnika. Iznimno je važno da poveznice u *spam* porukama ne slijedite.



Jačanjem svijesti korisnika o sigurnosnim pitanjima elektroničke pošte, a time i njihovog opreza, kriminalci se okreću ekskluzivnim ponudama ne bi li nas ipak dovoljno zaintrigirali. Suvremene prijevare nudit će nam izravno lijekove koji se inače izdaju po liječničkoj preporuci ili neobjavljeni videomaterijal o kojem mediji nagađaju.

JE LI VUK POJEO BANKU?

Trgovina i prijenos novca putem Interneta svakodnevna su pojava. Razumno je očekivati da gdje ima novca ima i kriminalaca koji će ga pokušati ukrasti.

Kriminalce zanimaju naše kreditne kartice i pristup uslugama vezanima uz novac.

Your credit/debit card information must be updated

Dear eBay Member,
We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you
The login attempt was made from:
IP address: 172.25.210.66
ISP Host: cache-66.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system o help you evaluate with who you are dealing with.

click on the link below, fill the form and then submit as we will verify
http://www.ebay.com/aw-cgi/eBayISAPI.dll?VerifyRegistrationShow
Please save this fraud alert ID for your reference

Please Note - If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

* Please do not respond to this e-mail as your reply will not be received.

Respectfully,
Trust and Safety Department
eBay Inc.

Helpful links
Search eBay - Find other items of interest
My eBay - Track your buying and selling activity
Discussion boards - Get help from other eBay members
eBay Help - Find answers to your questions

Learn More: Get notifications right on your desktop before an auction ends with the eBay Toolbar !

TaylorMade
IKEA BMW Nike
John Deere
Find it on ebay
Buy in Bulk and Save More!

Trading guidelines
eBay will not request personal data (password, credit card/bank numbers, and so on) in an email. Learn how to protect your account.

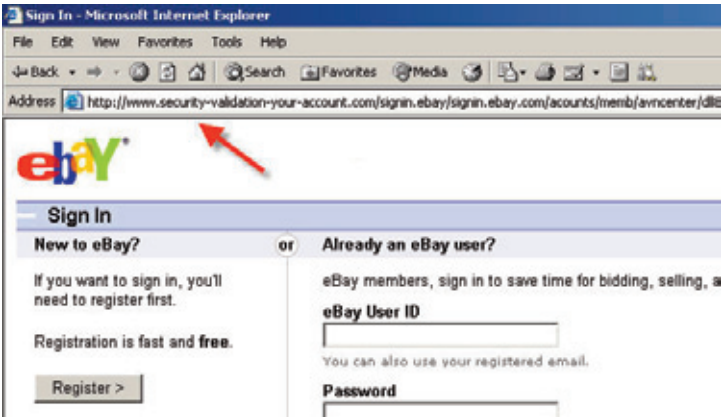
Thank you for using eBay!
http://www.ebay.com/

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Copyright © 2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.

eBay and the eBay logo are trademarks of eBay Inc.

Autor ove prijevare želi navesti korisnika da klikne na link iz poruke i tako ode na krivotvorenu stranicu s formularom za unos povjerljivih podataka



Primjetite li da se formular nalazi na HTTP, umjesto na HTTPS stranici, odmah možete znati da vašim povjerljivim podacima ovdje nije mjesto

Ne, ja sam Pero Korisnik

Pri svakom korištenju neke usluge putem Interneta dokazujemo svoj identitet. Uobičajeno to činimo unošenjem korisničkog imena i zaporke. Sazna li netko drugi te naše pristupne podatke, može u naše ime koristiti uslugu - dogodila nam se **krađa identiteta**.

Pretpostavimo li da nećemo svojevoljno odati svoje pristupne podatke, kako do njih kriminalci dolaze? Evo nekih od načina.

1. Jednostavno vas pitaju. U poruci elektroničke pošte, predstavljajući se kao vaš davatelj usluge, zatraže da potvrdite svoje pristupne podatke zbog nekog izmišljenog razloga.

2. Porukom elektroničke pošte koja govori o novostima i nudi poveznicu na službenu stranicu vašeg davatelja usluge. Zapravo vas vodi na imitaciju te web stranice koja pohranjuje vaše pristupne podatke.
3. *Spyware* na vašem računalu zapisuje sve zaporke koje upisujete i šalje ih svom tvorcu.
4. *Otmicom* prave adrese vašeg davatelja usluge i postavljanjem imitacije njegove web stranice.

Prva tri načina prikupljanja podataka zovemo ***phishing*** (eng. *fishing* - pecanje). Naziv dolazi od metode masovnog slanja prijevare i očekivanja rezultata korisnika koji su se "*upecali*".

Četvrti način događa se rjeđe, u slučajevima ozbiljnog narušavanja sigurnosti našeg pružatelja usluge. Takvi napadi obično traju vrlo kratko, no "*upecaju*" vrlo velik broj korisnika. Ovu metodu zovemo ***pharming*** (eng. *farming* - uzgoj na farmi).

Čuvajte svoje ja

Banke i institucije čija je sigurnost od iznimne važnosti koriste posebne uređaje dodijeljene u svrhu dokazivanja identiteta (**čitači kartica, *tokeni***). Ti uređaji pri kreiranju pristupnih podataka koriste ugrađeni tajni broj. Budući da taj broj nikada ne stigne do računala, kriminalci ga ne mogu ukrasti. Imate li izbora, birajte usluge koje koriste ovakve uređaje.

Tajni podaci, kao što su vaša zaporka, PIN, kontrolni kod kreditne kartice i slično, isključivo su vaši i nitko ih od vas ne smije zatražiti. Jedina iznimka je upravo ona usluga za koju su ti podaci namijenjeni. Davatelj usluge nikada od vas neće tražiti vaše tajne podatke. Uočite li takvu poruku, sigurno se radi o prijevari.

Spam poruke primamljivim nas ponudama dovode i na lažne web trgovine, kojima je jedina svrha prikupiti podatke o našoj kreditnoj kartici. Podatke o svojoj kreditnoj kartici upisujte samo na provjerene stranice renomiranih web trgovina.

Prepoznajte tuđe *ja*

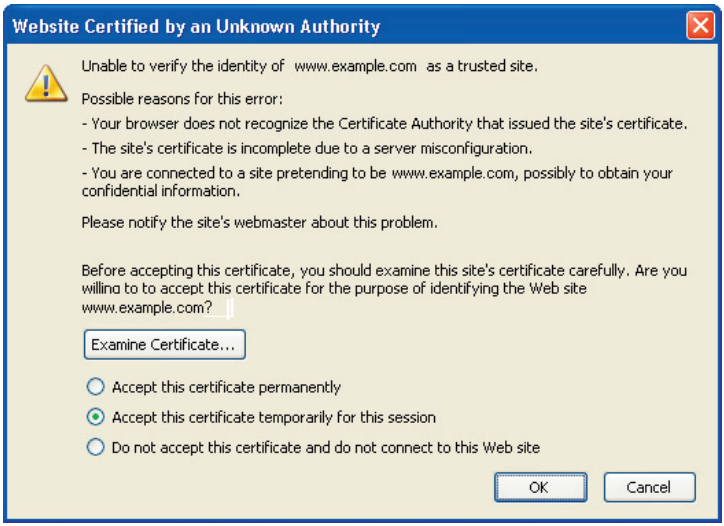
Uvijek pristupajte stranicama davatelja usluge ručnim upisivanjem adrese ili korištenjem pohranjene poveznice (*bookmark, favorite*). Ne slijedite poveznice u sumnjivim porukama da bi otkrili što iza njih stoji. Poruke s takvim poveznicama namjerno su nejasne ili nepotpune kako bi vas namamile da ih slijedite.

Koristite usluge isključivo onih davatelja čije web stranice zadovoljavaju osnovne sigurnosne standarde. To su:

1. Adresa stranice na kojoj upisujete povjerljive podatke mora započinjati prefiksom "https", a ne "http".
2. Web preglednik mora potvrditi ispravnost certifikata kojim web stranica dokazuje svoj identitet. Status certifikata vidljiv je kao sličica zatvorenog lokota u donjem desnom kutu prozora web preglednika.

3. Uz navedeno neki će web preglednici o ispravnosti certifikata obavijestiti i promjenom boje adresne trake.

Upozorenja web preglednika vezana uz certifikat nipošto nemojte ignorirati. Neispravan certifikat može značiti da se nalazite na web stranici koja je imitacija.



Primjer upozorenja kad je potrebno dodatno ispitati certifikat, jer web preglednik nije u mogućnosti automatski utvrditi njegovu vjerodostojnost.

IZGLEDA LI KAO PRIJEVARA I MIRIŠE NA PRIJEVARU

Čini li vam se nevjerojatnom srećom da ste baš vi dobili na lutriji (koju niste ni uplatili)? Izgleda li vam nevjerojatno da vas prijestolonasljednik zemlje za koju nikada niste čuli želi za posrednika u prijenosu milijunskog iznosa? Zvuči li vam besmisleno da ugledna tvrtka zahtijeva od svojih korisnika širenje obavijesti o novom virusu?

Gotovo svaka prijevara (***hoax***) započinje riječima "*zvučat će nevjerojatno, ali*". Tko ne bi bio pod iskušenjem da čak i najnevjerojatnijoj priči dâ šansu, ako se iza nje možda krije milijunska nagrada ili šansa da spasimo prijatelje od opasnog virusa?

Greška nastupa kada pomislimo da nemamo što izgubiti. Ponekad doista jest tako. Proslijedimo li lažnu obavijest na sve kontakte u svom adresaru, prijatelji će nam to vjerojatno oprostiti. S druge strane, odgovorimo li na lažnu lutriju ili priču o prijenosu velikog novca, uslijedit će vrlo opasne daljnje upute.

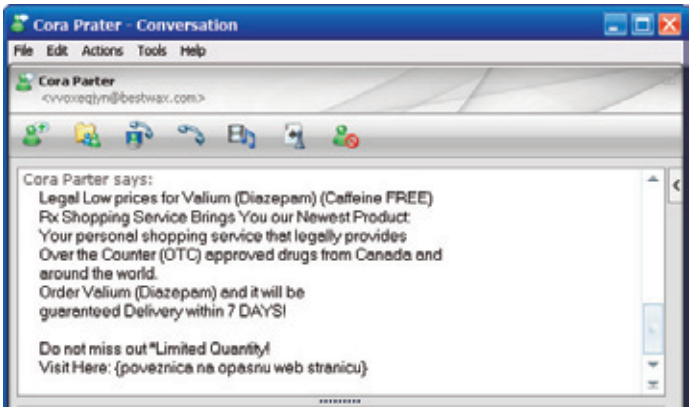
Vrlo stvarna opasnost

Pristanete li na igru kriminalaca koji stoje iza ***scamova***, najopasnijeg oblika prijevara, sigurno ćete izgubiti novac. Koristeći velik iznos kao mamac, tražit će od vas naizgled sitne "*prijenosne naknade*" i slične izmišljene namete, ne bi li iz vas izvukli što je moguće više. Ti zahtjevi trajat će sve do trenutka dok ih ne prestanete ispunjavati.

Novac možete gubiti i na međunarodnim pozivima na koje ste upućeni u prijevarama. Radi se o brojevima s iznimno visokim tarifama, kao u slučaju dialera.

Osim novca, na kocku može doći i vaša osobna sigurnost. Neke prijevare uključivale su pozive za dolazak u stranu zemlju (Nigerija je čest primjer), u kojoj su žrtve nasilno oplja-čkane ili otete. Iza scamova se kriju okorjeli kriminalci i njihovu opasnost treba shvatiti ozbiljno.

Protiv svih oblika socijalnog inženjeringa najbolja je obrana razum i zdrava doza sumnje. Primimo li poruku u kojoj nas netko pokušava u nešto uvjeriti ili nagovoriti, najmanje što trebamo učiniti je provjeriti njezine tvrdnje. Niste li sigurni u istinitost neke ponude, provjerite je koristeći neovisan izvor - potražite na Internetu gdje se sve spominju korištene ključne riječi. O prijevarama (*hoax*) se možete informirati i na stranicama CARNet CERT-a (http://www.cert.hr/hoax).



Osim elektroničkom poštom, spam i prijevare šire se i IM porukama.

Subject: AOL and Microsoft Merger....

I am forwarding this because the person who sent it to me is a good friend and does not send me junk. Microsoft and AOL are now the largest Internet company and in an effort make sure that Internet explorer remains the most widely used program, Microsoft and AOL are running an e-mail beta test. When you forward this e-mail to friends, Microsoft can and will track it (if you are a Microsoft Windows user) for a two week time period. For every person that you forward this e-mail to, Microsoft will pay you $245.00, for every person that you sent it to that forwards it on, Microsoft will pay you $243.00 and for every third person that receives it, you will be paid $241.00. Within two weeks, Microsoft will contact you for your address and then send you a check. I thought this was a scam myself, but two weeks after receiving this e-mail and forwarding it on, Microsoft contacted me for my e-mail and within days, I received a check for $24800.00. Name of an individual listed here FCG Inc. Wayne PA 610 225 xxxx xxxxxx@fcg.com

U jednoj od najdugovječnijih lančanih poruka, autor nas nagovara da poruku prosljeđujemo koristeći izmišljenu novčanu naknadu kao mamac.

PRIPREMA BOJIŠTA

USPOSTAVLJANJE PRVE LINIJE

Prije prvog spajanja računala na Internet nužno ga je zaštititi vatrozidom. Koristite li *Windows XP* s ugrađenim servisnim dodatkom *Service Pack 2*[1] , već imate *Windows Firewall*.

Windows Firewall pruža dovoljnu zaštitu da bez straha posjetite web stranice proizvođača nekog drugog vatrozida i preuzmete ga *(download)* na svoje računalo. Preporučamo vam ***ZoneAlarm***, dostupan na web adresi http://www.zonealarm.com.

U idealnom slučaju vatrozid ćete ugraditi bez spajanja računala na Internet. *ZoneAlarm* vatrozid nalazi se na CD mediju distribuiranom uz ovu brošuru. Ako nemate ni taj CD ni ugrađen *Windows Firewall*, preuzmite *ZoneAlarm* s Interneta koristeći neko drugo, već osigurano računalo. Nakon preuzimanja, datoteku dostavite na svoje računalo koristeći neki prenosivi medij.

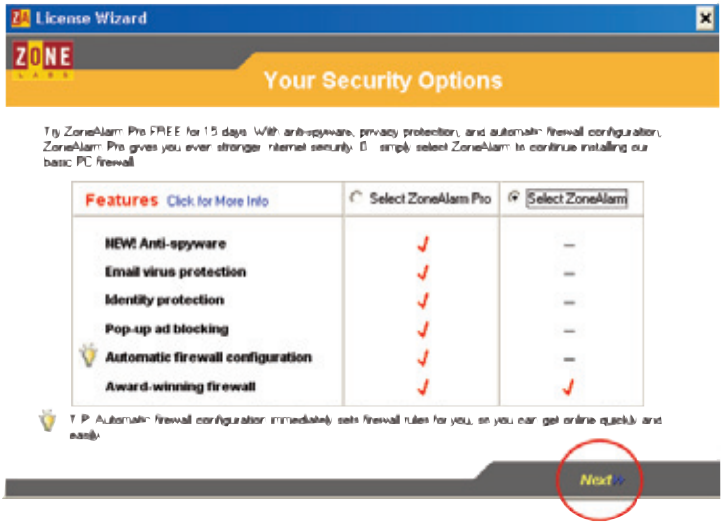
[1]Inačicu Windows operativnog sustava možete ustanoviti na sljedeći način: kliknite na *Start*, zatim na *Run* i u novootvoreni prozor upišite *"winver"* te kliknite na *OK*.

Ugradnja ZoneAlarm vatrozida

Nakon preuzimanja *ZoneAlarma* s web stranica proizvođača, pokrenite preuzetu datoteku.

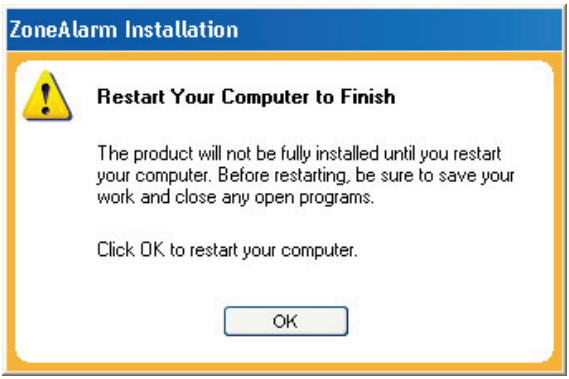
1. Slijedite upute čarobnjaka za instalaciju.
2. Po želji ispunite korisničku anketu ("*User survey*") ili jednostavno kliknite na *Finish*.

3. Potvrdite (kliknite na *Yes*) da želite odmah pokrenuti *ZoneAlarm*.



4. Odaberite opciju "*Select ZoneAlarm*" i kliknite na *Next*.

5. Kliknite na *Finish*, opet na *Finish* i zatim na *Done*.



6. Kliknite na *OK* da biste ponovno pokrenuli računalo.
7. Nakon ponovnog pokretanja računala, kliknite na "*No, thank you*" i zatim na *Finis*h.

ODABIR DIPLOMATA

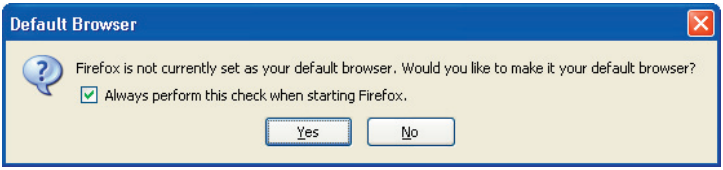
Programi kao što su web preglednik ili klijent elektroničke pošte kontinuirano su izloženi opasnom sadržaju s Interneta. Sjetimo se, korištenjem alternativnih programa za ovu namjenu smanjujemo izloženost tim opasnostima.

Najizloženiji program koji odgovara ovom opisu je web preglednik. Većina spywarea, adwarea i trojanskih konja nalazi svoj put na naše računalo upravo kroz njega. Zamijenimo ga nekom od alternativa:

Mozilla Firefox (http://www.getfirefox.com) - drugi web preglednik po zastupljenosti[1], vrlo pristupačan

Opera (http://www.opera.com) - iznimno siguran web preglednik, nešto manje zastupljen i namijenjen iskusnijim korisnicima

Web preglednike *Mozilla Firefox* i *Opera* možete pronaći na CD mediju distribuiranom uz ovu brošuru, ili ih preuzeti s navedenih web adresa. Nakon preuzimanja jednostavno pokrenite preuzetu datoteku i slijedite upute čarobnjaka.

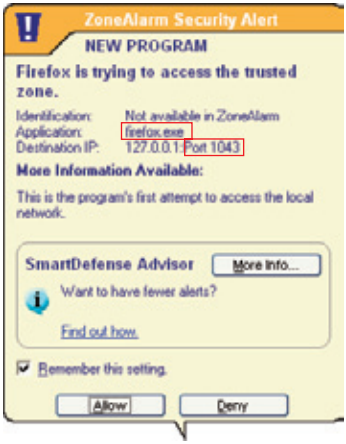


Prvo pokretanje *Mozilla Firefoxa* rezultirat će pitanjem želimo li ga koristiti kao standardni web preglednik. To znači da će se *Mozilla Firefox* automatski pokretati kada neki drugi program zatraži prikaz web stranice.

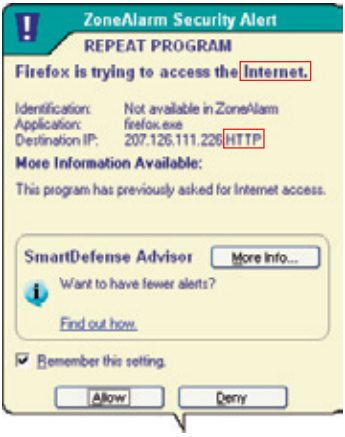
[1]manje zastupljeni web preglednici poneke web stranice ne prikazuju ispravno; autori web stranica obično provjeravaju ispravnost prikaza u jednom ili dva najzastupljenija proizvoda

Nakon ugradnje Mozilla Firefox web preglednika

Novi web preglednik ugrađen u računalo vaš vatrozid još ne poznaje. Pokušaj web preglednika *Mozilla Firefox* za komunikacijom rezultirat će upozorenjem:



Mozilla Firefox za rad koristi i komunikaciju unutar računala



Mozilla Firefox pristupa Internetu.

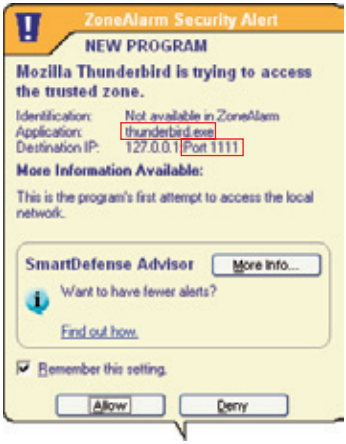
"HTTP" u drugom pitanju vatrozida odnosi se na komunikacijski port, odnosno naziv usluge koja se putem tog porta ostvaruje. Web preglednik u svakodnevnom radu koristi HTTP, HTTPS i DNS (bilo koji od ovih naziva usluge mogu se pojaviti u drugom pitanju vatrozida).

Odgovaraju li pitanja vatrozida ovim prikazima (uočite napomenu o nazivima usluga u drugom pitanju!), označite kvadratić pored opcije "*Remember this setting*" i kliknite na *Allow*. Na taj će način *ZoneAlarm* vatrozid zapamtiti da *Mozilla Firefox* smije pristupati Internetu.

Alternativa za elektroničku poštu

Koristite li klijent elektroničke pošte kao što je *Outlook Express*, također vam preporučamo alternativu - *Mozilla Thunderbird*.

Klijent elektroničke pošte *Mozilla Thunderbird* možete preuzeti s web adrese http://www.getthunderbird.com. Preuzetu datoteku pokrenite i slijedite upute čarobnjaka za instalaciju[1].



Mozilla Thunderbird za rad koristi i komunikaciju unutar računala

Mozilla Thunderbird pristupa Internetu.

"POP3" se u drugom pitanju odnosi na naziv usluge, kao i u slučaju *Mozilla Firefoxa*. Usluge koje *Mozilla Thunderbird* u uobičajenom radu koristi su POP3 i SMTP (u nekim slučajevima koriste se portovi 995 i 465).

[1]detaljne upute za podešavanje elektroničke pošte zatražite od svog pružatelja usluge

RAZMJEŠTANJE TRUPA

Osnova naše obrane protiv nametnika je antivirusni alat. Na tržištu postoje besplatni[1] programi ove namjene koji od korisnika zahtijevaju samo jednogodišnju registraciju. Preporučujemo vam *avast!* (http://www.avast.com) ili AVG (http://www.grisoft.com/).

Namjeravate li koristiti P2P, IM ili klijent elektroničke pošte, ugradite te programe u računalo neposredno prije antivirusnog alata.

(!) Antivirus i anti-spyware alati će odmah po završetku ugradnje tražiti pristup Internetu. Pobrinite se da vam je računalo nakon svakog ponovnog podizanja sustava spojeno na Internet.

(!) Pri ažuriranju alata javljat će se upozorenja vatrozida, kao i u slučaju web preglednika. Postupite na već opisan način da bi se ažuriranje moglo nesmetano odvijati.

Ugradnja i podešavanje avast! antivirusnog alata

1. Na CD-u uz brošuru ili web stranici http://www.avast.com pronađite i preuzmite avast! Home Edition (English).
2. Na istoj web stranici pronađite poveznicu na formular za registraciju i ispunite ga[2].
3. Nakon preuzimanja datoteke (iz koraka 1.), pokrenite datoteku i slijedite upute čarobnjaka.

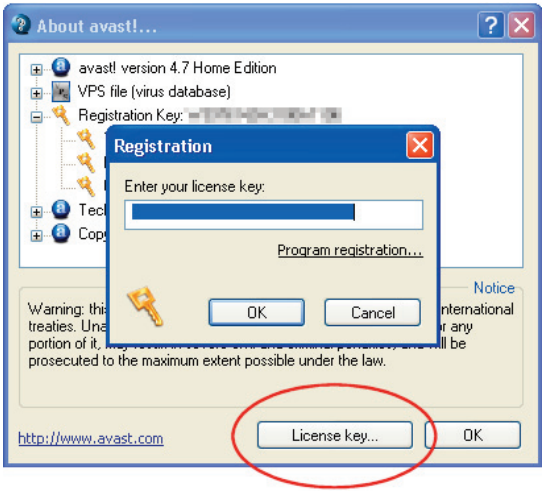
Nakon ugradnje

Za ispravan rad antivirusnog alata ključne su uvijek ažurne antivirusne definicije i inačica jezgre antivirusnog alata. Da biste koristili funkciju automatskog ažuriranja, potrebno je unijeti registracijski kod dobiven nakon ispunjavanja web formulara.

[1]za kućnu uporabu; [2]za registraciju morate imati na raspolaganju adresu elektroničke pošte; ne znate li svoju adresu, obratite se podršci vašeg pružatelja Internetske usluge i pitajte za adresu elektroničke pošte koja vam je dodijeljena uz pristup Internetu

1. Provjerite elektroničku poštu, pronađite poruku naziva "*avast! Registration*" i kopirajte *(Copy, CTRL+C)* dobiveni registracijski kod.

2. U donjem desnom uglu ekrana pronađite plavu ikonu sa slovom a i kliknite na nju desnom tipkom miša. Iz izbornika izaberite stavku "*About avast!...*".



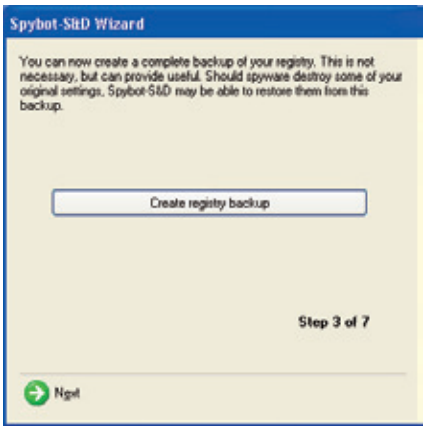
3. Kliknite na "*License key*" i zalijepite *(Paste, CTRL+V)* registracijski kod. Kliknite na *OK.*

Anti-spyware

Od *spywarea, adwarea* i *dialera* štite nas anti-spyware alati. Budući da se radi o nametnicima koje je najteže prepoznati i iskorijeniti, koristimo kombinaciju dvaju popularnih besplatnih alata.

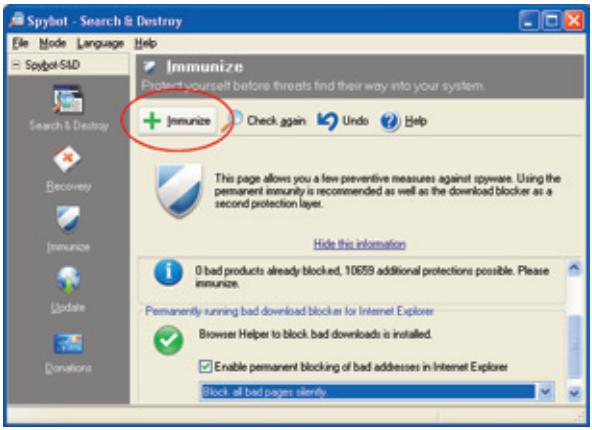
Spybot - Search & Destroy (http://www.safer-networking.org)
Ad-Aware (http://www.lavasoftusa.com)

1. Na CD-u uz brošuru ili web stranici http://www.safer-networking.org pronađite i preuzmite *Spybot - Search & Destroy*.
2. Pokrenite preuzetu datoteku i slijedite upute čarobnjaka za instalaciju.
3. Pri prvom pokretanju Spybot Search & Destroy, pojavljuje se čarobnjak za instalaciju. Slijedite sve preporučene korake:



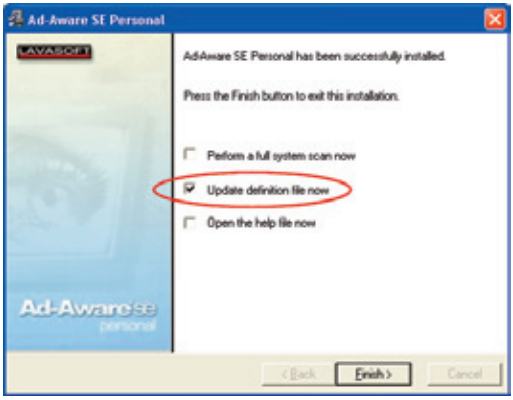
3a. *"Create registry backup"*. Nakon završetka procesa, kliknite na *Next*.
3b. *"Search for updates"*.
3c. *"Download all available updates"*.

4. Kliknite na sličicu *Immunize*. Kliknite na OK.



5. Kliknite na *Immunize* u desnom dijelu prozora.
6. Zatvorite *Spybot - Search & Destroy.*

1. Na CD-u uz brošuru ili web stranici http://www.lavasoftusa.com pronađite i preuzmite *Ad-Aware SE Personal*.
2. Pokrenite preuzetu datoteku i slijedite upute čarobnjaka za instalaciju.



3. Na posljednjem koraku čarobnjaka ostavite uključenu samo opciju "*Update definition file now*" i kliknite na *Finish*. Pričekajte da ažuriranje završi.

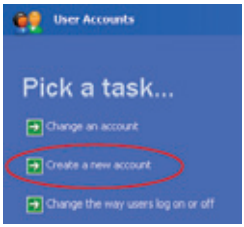
ODRŽAVANJE PRIPRAVNOSTI

Neprijatelj nikada ne spava. Iz sata u sat kriminalci smišljaju nove načine na koje mogu zaobići sigurnosnu zaštitu našeg računala ili iskoristiti neku novootkrivenu ranjivost. No nismo ni mi bespomoćni. Održavamo li sve naše linije obrane ažurnima i pripravnima, naša izloženost opasnosti bit će minimalna.

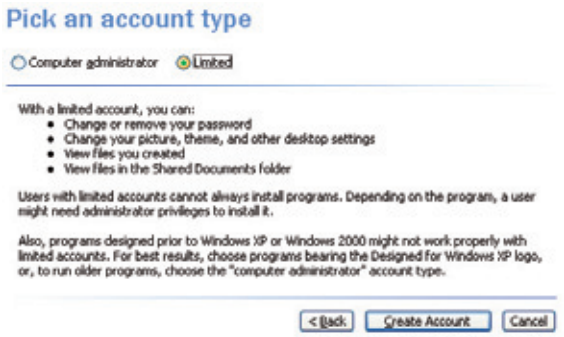
Kontrolna soba

U svakodnevnom radu s računalom nisu nam potrebne mogućnosti mijenjanja njegovih postavki, kao ni dodavanja i uklanjanja programa i slično. Oduzmemo li sebi te mogućnosti u slučajevima kada nam ne trebaju, oduzeli smo ih i nametnicima koji se za vrijeme našeg rada probijaju na računalo.

1. Kliknite na *Start,* zatim na *Control Panel* pa na *User Accounts*.



2. Kliknite na *"Create a new account"*.
3. Unesite ime pod kojim ćete svakodnevno raditi. Kliknite na *Next.*

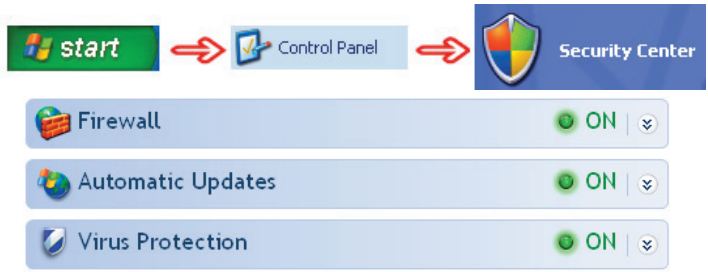


4. Označite opciju *"Limited"* i kliknite na *Create account*.

Ime koje ste upravo unijeli pojavit će se na početnom zaslonu prilikom podizanja operativnog sustava. Počnite se koristiti tim imenom tek u svakodnevnom radu, kada je vaše računalo potpuno podešeno i sve sigurnosne aplikacije ugrađene.

Windows Security Center

Windows XP Service Pack 2 ima ugrađen mehanizam praćenja sigurnosnih alata i njihove ažurnosti, kao i ažurnosti samog Windows operativnog sustava. Provjerimo uz njegovu pomoć je li naše računalo ispravno osigurano.



Odgovara li stanje prikazano u *Windows Security Centeru* ovome na slici, naše računalo je ispravno ažurirano i zaštićeno.

Windows Security Center prati za nas samo pet jednostavnih, ali vrlo važnih informacija:

1. Vatrozid je uključen
2. Automatsko ažuriranje je uključeno i ispravno podešeno
3. Na računalo je ugrađen antivirusni alat
4. Antivirusni alat je uključen
5. Antivirusni alat koristi ažurne virusne definicije

Windows Security Center ne prati stanje anti-spyware alata ni alternativnih aplikacija.

Ažuriranje preporučenih programa

Među preporučenim programima i alatima, jedino *ZoneAlarm* nema mogućnost samoažuriranja. *ZoneAlarm* povremeno provjerava postoji li novija inačica te upućuje korisnika da je preuzme sa stranica proizvođača.

Vatrozid nakon ažuriranja više ne prepoznaje web preglednik *Mozilla Firefox*, što znači da će se vatrozid ponašati kao kod prve ugradnje, postavljajući ponovno ista pitanja. *Mozilla Thunderbird*, ako ste ga ugradili, ponaša se na jednak način.

Avast! antivirus pri ažuriranju svoje jezgre također se izmjeni i vatrozid ga više ne prepoznaje. Potrebno je ponovno odgovoriti na pitanja vatrozida.

Spybot - Search & Destroy i *Ad-Aware* ažuriraju se i pokreću na zahtjev korisnika. Ažuriranje je kod oba alata dostupno već u osnovnom prozoru.

CIVILI NA SIGURNOM

Postavljanje računala postupak je koji često oduzima mnogo vremena. Kako bi u slučaju gubitku podataka što prije ponovno bili spremni za rad, poželjno je izraditi sigurnosnu kopiju operativnog sustava.

Kako bi sigurnosna kopija zauzimala što manje diskovnog prostora, prije izrade s diska ćemo ukloniti podatke koji za sam operativni sustav nisu važni. Ukoliko ste računalo tek nabavili i postavljate ga upravo sada, dok čitate ovaj tekst, naredna 2 koraka možete preskočiti i odmah nastaviti s *"izradom sigurnosne kopije operativnog sustava"*.

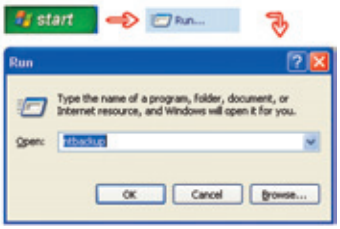
1. Gdje se sve nalaze podaci koji su vam važni? Pronađite i zapišite sva mjesta.

2a. Imate li na računalu više od jednog čvrstog diska ili logičke jedinice, prebacite važne podatke na to mjesto (uklanjajući ih s izvorne lokacije).

2b. Nemate li takvu mogućnost, prebacite važne podatke na CD, DVD ili prenosivi čvrsti disk (uklanjajući ih s izvorne lokacije).

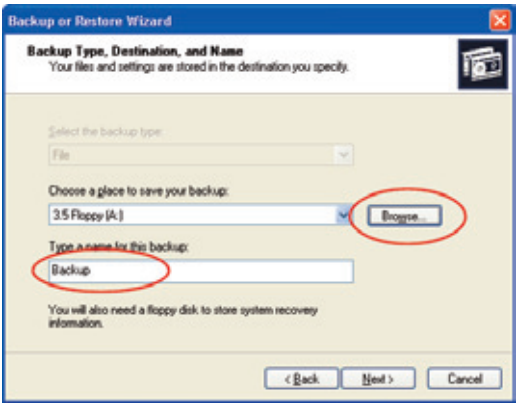
Izrada sigurnosne kopije operativnog sustava

Ako je uz vaše računalo isporučen program za izradu sigurnosne kopije čitavog diska, upotrijebite ga. U suprotnom, upotrijebite *NTBackup*.



1. Kliknite na *Start*, zatim na *Run*, upišite *NTBackup* te kliknite na *OK*.

2. Pokrenuli ste čarobnjak za *backup*. Kliknite na *Next.*
3. Odaberite *"Back up files and settings"*. Kliknite na *Next.*
4. Odaberite "*All information on this computer*". Kliknite na *Next.*



5. Kliknite na *Browse* i odaberite lokaciju na koju ćete privremeno pohraniti sigurnosnu kopiju.
6. U prozor na označeno mjesto upišite ime sigurnosne kopije (npr. ime računala i današnji datum). Kliknite na *Next.*
7. Kliknite na *Finish* (proces koji slijedi iznimno je dugotrajan)
8. Pripremite praznu disketu i slijedite upute.
9. Privremenu datoteku pohranite na siguran prenosivi medij i uklonite s računala.

Arhivske kopije multimedije

Fotografije, audio i videozapise te nepromjenjive dokumente (*.pdf*) osim na računalo uvijek pohranjujte i na prenosive medije. Na taj način bez brige možete brisati krupne sadržaje s računala kada vam ponestane prostora.

Multimedija je krupan i nepromjenjiv sadržaj, zbog čega se ne bi trebala miješati s dokumentima koje svakodnevno uređujemo. Jedan od načina je da za multimedijalne i slične sadržaje koristimo mapu *Shared Documents*. Ova mapa dostupna nam je i korištenjem ograničenog pristupa računalu (vidi *"Kontrolna soba"*, str. 41).

Iz dana u dan

Za dokumente koje mijenjamo svakodnevno, čak i jedan dan gubitka može značiti veliku štetu. Srećom, količina prostora koju obično zauzimaju takvi podaci vrlo je mala i nije je teško pohraniti. Držimo li sve dokumente ovog tipa unutar naših korisničkih mapa, kao što su *My Documents* i *Desktop,* dovoljno je uz pomoć *NTBackup* programa redovito pohranjivati korisnički profil.

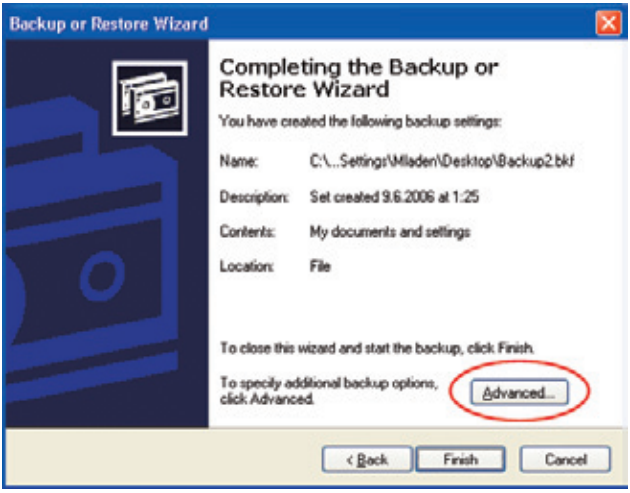
Strategija izrade sigurnosnih kopija promjenjivih podataka uključuje povremenu izradu kompletnih kopija *(Normal backup)* i često pohranjivanje razlika nastalih od posljednje kompletne kopije *(Differential backup)*. Izradimo prvo kompletnu kopiju.

1. Kliknite na *Start*, zatim na *Run*, upišite *NTBackup* te kliknite na *OK*.
2. Pokrenuli ste čarobnjak za *backup*. Kliknite na *Next*.
3. Odaberite "*Back up files and settings*". Kliknite na *Next*.
4. Odaberite "*My documents and settings*". Kliknite na *Next*.
5. Kliknite na *Browse* i odaberite lokaciju na koju ćete privremeno pohraniti sigurnosnu kopiju.
6. U prozor na označeno mjesto upišite ime sigurnosne kopije (npr. *"profil"* i današnji datum). Kliknite na *Next*.
7. Kliknite na *Finish* i pričekajte nekoliko minuta.

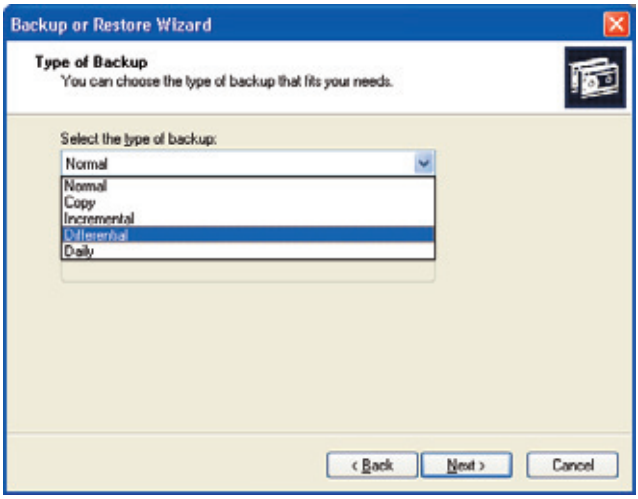
8. Privremenu datoteku pohranite na siguran prenosivi medij i uklonite s računala.

Nakon što ste učinili važne izmjene na svojim dokumentima i želite napraviti sigurnosnu kopiju, potrebno je pohraniti samo mijenjane datoteke.

1. Kliknite na *Start*, zatim na *Run*, upišite *NTBackup* te kliknite na *OK*.
2. Pokrenuli ste čarobnjak za *backup*. Kliknite na *Next.*
3. Odaberite *"Back up files and settings"*. Kliknite na *Next.*
4. Odaberite *"My documents and settings"*. Kliknite na *Next.*
5. Kliknite na *Browse* i odaberite lokaciju na koju ćete privremeno pohraniti sigurnosnu kopiju.
6. U prozor na označeno mjesto upišite ime sigurnosne kopije (npr. *"profil_diff"* i današnji datum). Kliknite na *Next.*



7. Kliknite na *Advanced*



8. Iz padajućeg izbornika izaberite *Differential*. Kliknite na *Next*.
9. Kliknite na *Next* još 3 puta. Kliknite na *Finish* i pričekajte.
10. Privremenu datoteku pohranite na siguran prenosivi medij i uklonite s računala.

Diferencijalne sigurnosne kopije nastaju vrlo brzo i njihova veličina obično ne predstavlja problem. Izrađujte ih i pohranjujte svaki put kada su vam netom učinjene izmjene dragocjene.

S vremenom će se razlika između prethodne kompletne sigurnosne kopije i aktualnog stanja povećati (što znači da će diferencijalne kopije postati veće). Kada se to dogodi, napravite novu kompletnu sigurnosnu kopiju.

POJMOVNIK

adware - (eng. *ad* - oglas) program namjenjen prikazivanju reklamnog sadržaja, uglavnom bez pristanka korisnika

alternativni programi - programi koji zamjenjuju unaprijed ugrađene ili najrasprostranjenije programe

anti-spyware alat - program specijaliziran za uklanjanje *spywarea, adwarea* i *dialera*

antivirusni alat - program namjenjen uklanjanju i sprječavanju rada malicioznog koda

automatic update - (eng. *automatic update* - automatsko ažuriranje) postupak preuzimanja s Interneta i ugradnje novijih inačica programa i komponenti bez korisničke intervencije

backup - (eng. *backup* - pričuva ili zamjena) pričuvna kopija važnih podataka; također postupak stvaranja pričuvnih kopija

bežična lokalna mreža - (eng. *WLAN, Wireless Local Area Network*) mreža računala povezanih radio-signalom na malim udaljenostima

bežična veza - (eng. *wireless connection*) veza između računala ostvarena pomoću radio-signala na proizvoljnoj udaljenosti

crv - (eng. *worm*) maliciozni računalni kod koji se širi kopiranjem svojeg cjelokupnog sadržaja kroz neki medij komunikacije, npr. elektroničku poštu; tipičan su primjer crvi u obliku privitaka porukama elektroničke pošte

dialer - (eng. *dial* - birati [telefonski broj]) program namjenjen povezivanju računala putem *dial-up* veze; u praksi se uglavnom radi o prekidanju veze s vašim ISP-om i uspostavljanju skupe međunarodne veze

dial-up - međusobno povezivanje računala telefonskim pozivom

DSL - brza veza između računala ostvarena putem telefonske linije; protok podataka odvija se neovisno o telefonskim pozivima

IM - (eng. instant messaging) trenutna razmjena tekstualnih poruka između korisnika putem interneta.

IP adresa - jedinstvena brojčana adresa na nekoj mreži, kao što je Internet (npr. adresa CERT-ovog web poslužitelja je 161.53.160.69)

ISP - (eng. *Internet Service Provider* - pružatelj Internet usluge) organizacija koja omogućava spajanje računala na Internet (poznata još i kao Internet operater)

kablovski Internet - usluga spajanja na Internet putem infrastrukture primarno namjenjene distribuciji TV signala (mreže kablovske televizije)

komunikacijski port - (lat. *portus* - vrata) brojčana oznaka koja dogovorno određuje vrstu mrežne usluge (npr. port 80 koristi se za web stranice)

krađa identiteta - (eng. *identity theft*) prikupljanje kombinacije nečijih osobnih informacija dovoljne za predstavljanje u ime te osobe (npr. korisničko ime i zaporka)

malware - skupni naziv za sve oblike malicioznog koda

P2P - (peer-to-peer) izravna razmjena datoteka između korisnika putem interneta.

pharming - postupak masovne krađe identiteta presretanjem komunikacije između korisnika i legalnog poslužitelja

phishing - postupak masovne krađe identiteta (vidi *krađa identiteta*) socijalnim inženjeringom (vidi *socijalni inženjering*)

prijevara - (eng. *hoax*) poruka koja zastrašivanjem ili manipuliranjem pokušava pridobiti korisnika da je proširi; opasniji oblici nagovaraju korisnike na opasne ili čak ilegalne radnje (vidi *scam, phishing*)

privitak - (eng. *attachment*) datoteka - dodatak poruci elektroničke pošte, obično netekstualnog sadržaja

scam - prijevara smišljena u cilju ostvarivanja materijalne dobiti ilegalnim aktivnostima

socijalni inženjering - (eng. *social engineering*) manipulacija korisnika lažnim tvrdnjama i zastrašivanjem kako bi ih se pridobilo da zaobiđu sigurnosnu zaštitu ili otkriju povjerljive podatke

spam - neželjene, obično reklamne poruke koje se distribuiraju nerazmjerno velikom broju korisnika

spyware - (eng. *spy* - špijunirati) program namjenjen praćenju i bilježenju korisnikovih aktivnosti te povjerljivih podataka kao što su zaporke

trojanski konj - (eng. *trojan horse*) maliciozni računalni kod koji lažnim predstavljanjem pokušava pridobiti korisnika da mu omogući izvršavanje (npr. lažne računalne igre slane u obliku privitka poruci elektroničke pošte)

vatrozid - (eng. *firewall*) program koji kontrolira ulaz i izlaz podataka putem mreže

virus - maliciozni računalni kod koji se širi dodavanjem svojeg koda drugim aplikacijama; pokretanjem "zaražene" aplikacije aktivira se i kod virusa

web defacement - (eng. *web defacement* - obezličenje web stranice) vandaliziranje sadržaja web stranice izmjenom i/ili dodavanjem provokativnih poruka; neovlašten pristup događa se uslijed kompromitiranja sigurnosne zaštite poslužitelja na kojem se web sadržaj nalazi

Izdavač:
Hrvatska akademska i istraživačka mreža CARNet
Josipa Marohnića 5, Zagreb
tel: 01 6661 616, fax: 01 6661 615
http://www.carnet.hr