
LOGOSOFT
KAKO SE ZAŠTITI
NA INTERNETU

Sadržaj

Iako je do vašeg računara ponekad moguće doći i bez vašeg odobrenja, većinom su vaše odluke prva i posljednja linija odbrane. Vaša svijest o informacijskoj sigurnosti najbolji je sigurnosni alat. –Slijedite li preporuke sigurnosnih stručnjaka i donosite li informisane odluke o vjerodostojnosti sadržaja koji vam se nudi na Internetu, predstavljate tvrd orah za prevarante te će vas većina jednostavno zaobići u potrazi za lakšom žrtvom.

Na tehničkom nivou, računar je potrebno zaštititi odgovarajućim sigurnosnim softverom te ispravnim podešavanjima operativnog sistema i aplikacija.

Izdvojit ćemo najvažnije elemente zaštite, softver koji biste trebali imati i pravila kojih se treba dobro držati.

Softver

Vrlo je važno koristiti legalan i licenciran softver, jer samo tako možete biti sigurni u njegovu ispravnost i da će biti redovno ažuriran. To se odnosi kako na aplikacije koje koristite u radu ili za zabavu, tako i na one koje su tu da vas zaštite od zlonamjernog djelovanja.

Softveri za zaštitu

Antivirusni alat je obavezan dio softverske opreme vašeg računara. Neka rješenja dolaze u paketima sa drugim sigurnosnim softverom (npr. firewallom), dok su neka samostalna. ***Windows Security Center*** provjerava prisutnost i ispravan rad antivirusnog softvera te će u slučaju problema korisnika upozoriti crvenim štitom u statusnoj traci (system tray). Preporučeno besplatno rješenje je ***Avast!*** antivirus.

Firewall je aplikacija koja ograničava mrežnu komunikaciju između vašeg računara i Interneta; selektivnim propuštanjem saobraćaja izbjegava se neovlaštena komunikacija i smanjuje mogućnost iskorištenja sigurnosnih propusta u aplikacijama koje imaju mogućnost mrežne komunikacije.

Windows operativni sistem (XP i noviji) po ugradnji u računar već sadrži firewall s odgovarajućom zaštitom. Firewall će vas upitati za odobrenje svaki puta kada neka nova aplikacija pokuša poslati podatke putem mreže.

Važnost podešavanja i ažuriranja operativnog sistema i aplikacija

Sigurnosni propusti u softveru stalno se otkrivaju. Kako vas ne bi ostavili ranjivima, uključite automatsko ažuriranje u operativnom sistemu i svim aplikacijama koje dolaze u kontakt sa sadržajima s Interneta (npr. čitači za PDF dokumente). ***Windows Security Center*** posmatra je li automatsko ažuriranje operativnog sistema uključeno te upozorava korisnika ako nije.

Korištenje korisničkog računa sa smanjenim privilegijama (*limited user account*)

Preporučljivo je da korisnički račun kojim se služite u svakodnevnom radu ima ograničen pristup računaru. Na taj način, većina malvera[1] (*Malware*) jednostavno neće imati pristup ključnim dijelovima operativnog sistema i neće moći obaviti svoj zadatak. Kada vam zatrebaju veće ovlasti, jednostavno se odjavite i prijavite ponovno kao korisnik Administrator, obavite što trebate i ponovno se prijavite sa svojim svakodnevnim korisničkim računom. Ukoliko dijete koristi isti računar, obavezno napraviti korisnički račun za njega/nju. O zaštiti djece opširnije ćemo govoriti u nastavku.

[1] *Malware* (skraćenica od *malicious software*, "zlonamjeran softver") je softverski program napravljen tako da se neprimjetno ubaci u sistem računara i načini neku vrstu štete. *Malware* može biti računarski virus, crv, trojanski konj, *spyware*, *adware* ili neki drugi štetni program.

UKRATKO
Za zaštitu na Internetu držite se sljedećih pravila

- ✓ Redovno ažurirajte operativni sistem, antivirusni softver i sve aplikacije koje dolaze u kontakt sa sadržajima s Interneta;
- ✓ Koristite enkripciju na kućnoj bežičnoj mreži;
- ✓ Koristite kompleksne lozinke za pristup javnim servisima (društvenim mrežama, elektronskoj pošti i sl.);
- ✓ Sve novčane transakcije, a posebno rad s e-bankarstvom, obavljajte s računara koje je najmanje izloženo riziku zaraze;
- ✓ Ne isključujte firewall i antivirusni softver i ne ignorišite njihova upozorenja;
- ✓ Prilikom instalacije besplatnih programa, dobro obratite pažnju šta piše na svakoj stranici tokom instalacije prije nego što pritisnete next ili install. Uz besplatne alate često se instaliraju dodatne aplikacije koje niste primijetili, koje ne želite i koje u sebi najčešće sadrže spyware ili neki drugi maliciozni softver;
- ✓ Klonite se stranica sa pornografskim i piratiziranim sadržajima. One su najčešći izvori virusnih zaraza računara;
- ✓ Koristite legalni softver.

Kako prepoznati opasnost

Kako bismo spriječili izvršavanje stranog koda na svom računaru, prvo moramo znati prepoznati situacije u kojima nas računar pita za dozvolu da se neki kod izvrši.

Web preglednik i operativni sistem će nas upozoriti u svakoj situaciji u kojoj se datoteke preuzete s Interneta trebaju izvršiti i dati nam priliku da to odbijemo. **Kako znati trebamo li dopustiti izvršenje ili ne?** Radi li se o iznenadnom upitu, odgovor je ne; dozvolu za izvršavanje trebamo dati isključivo aplikacijama koje želimo pokrenuti. Kod nekih web stranica postoji veća vjerojatnost da ćemo zateći maliciozan kod koji već prilikom prikaza stranice pokušava iskoristiti propuste u našem web pregledniku ili nas prevariti. Takav se kod može provući i kroz reklamni sadržaj na inače legitimnim web stranicama, no najčešće je prisutan na stranicama **pornografske tematike, neprovjerenim web kockarnicama i stranicama s piratiziranim materijalima (stranice za pruzimanje ilegalnog softvera, stranice za ilegalno preuzimanje filmova, serija i muzike),** zato izbjegavajte takve stranice**.**

Ponekad se opasne web stranice kriju iza izgleda koji imitira nama poznate servise, kao što je web mail ili društvena mreža koju koristimo. Obično ćemo na takvoj stranici završiti slijedeći link iz sumnjivog izvora. Važno je pogledati web adresu (URL) koja se u tom trenutku pojavljuje u adresnoj traci web preglednika.

Također, slijedimo li pravilo da na stranice koje redovno koristimo uvijek dolazimo iz vlastitih linkova ili upisivanjem adrese u adresnu traku, isključili smo mogućnost da smo "zalutali" na imitaciju. Imamo li sve ovo na umu, vjerojatno smo izbjegli većinu opasnosti, no kako prepoznati da je naš računar zaražen ako se to ipak dogodi? Malver se često stvara brže nego što to proizvođači antivirusnih alata mogu pratiti pa vaš računar može biti zaražen, a da to antivirus nije u mogućnosti prepoznati. Zato vodite računa da vam je antivirusni softver uvijek ažuriran.

Na žalost, nema garancije da će zaraženost biti moguće ustanoviti, no neki nam pokazatelji ipak mogu odati prisutnost malvera. Pojavljuju li se na računaru spontano alarmantni upiti, kao što je prozor s upozorenjem da će se računar uskoro ugasiti, vrijeme je za stručnu provjeru. Upišete li web adresu proizvođača sigurnosnog alata ili druge web stranice koju inače posjećujete, a umjesto nje se pojavi web trgovina ili oglašivački sadržaj, vaš računar je gotovo sigurno zaražen.

UKRATKO
o zaštiti djece na Internetu

- ✓ Educirajte se o servisima koje vaše dijete koristi;
- ✓ Postavite pravila korištenja računara;
- ✓ Smjestite računar u zajedničku prostoriju;
- ✓ Objasnite opasnosti interakcije s nepoznatim ljudima na Internetu, a pogotovo nalaženja s istim tim ljudima uživo;
- ✓ Saznajte kroz razgovor što je moguće više o Internet prijateljima vašeg djeteta;
- ✓ Objasnite važnost privatnosti i anonimnosti;
- ✓ Pratite aktivnosti djeteta na društvenim mrežama;
- ✓ Koristite softver za roditeljski nadzor;
- ✓ Budite svjesni posljedica postavljanja fotografskog i video sadržaja na Internet. Kada se takav sadržaj jednom postavi, teško da ćete ga ikada uspjeti skinuti, zato je veoma važno biti svjestan mogućih posljedica zbog onog što vaše dijete može da postavi na Internet kroz društvene mreže i alate za dijeljenje videa i slika.

Vodič za roditelje

Kao roditelj sigurno znate mnogo više od svog djeteta o stvarima s kojima se ono prvi put susreće u životu. Računari su jedan od primjera gdje gotovo sigurno nije tako. Čak i ako su računara vaša struka, vaše će dijete i dalje biti u prednosti zbog specifičnog načina na koji se njime koristi i područja interesa koje vjerojatno s njime ne dijelite. Zato uvijek preporučujemo korištenje softvera za roditeljsku kontrolu. Najrasprostranjeniji operativni sistem Windows od verzije Vista ima vlastiti softver namijenjen zaštiti djece na Internetu.

Family Safety (Windows Vista, Windows 7, Windows 8)

Family Safety predstavlja uslugu roditeljskog nadzora koja omogućava roditeljima da odrede sadržaj koji njihova djeca mogu da vide na mreži i kontakte sa kojima ona mogu da komuniciraju korištenjem usluga Windows usluga za chat (*Messenger*).

Usluga *Family Safety* obuhvata:

Filtriranje sadržaja
Roditelji mogu da preciziraju Web lokacije koje njihova djeca mogu da pregledaju, i po kategorijama sadržaja, i po URL adresi.

Izvještavanje o aktivnostima
Roditelji mogu da biraju da li žele da (na mreži ili putem e-pošte) pregledaju izvještaje o Web lokacijama koje su njihova djeca posjetila ili pokušala da posjete.

Ograničenje korištenja aplikacija
Roditelji mogu da izaberu da li njihova djeca mogu da koriste određene usluge na mreži.

Upravljanje kontaktima
Ukoliko je djeci dozvoljeno da koriste Windows Live usluge, roditelji mogu da izaberu kontakte s kojima djeca smiju da komuniciraju korištenjem ovih usluga.

Djeca mogu da traže od svojih roditelja da im dozvole pristup blokiranim Web lokacijama ili kontaktima.

Usluga *Family Safety* ne dijeli podatke o aktivnostima djeteta na mreži sa drugim proizvodima ili uslugama. Roditelji i djeca će primati e-mailove u sklopu uobičajenog načina funkcionisanja usluge .

Detaljno uputstvo za postavljanje i upravljanje *Family Safety* opcijom možete pronaći ovdje:

http://windows.microsoft.com/hr-hr/windows/set-up-family-safety#set-up-family-safety=windows-8