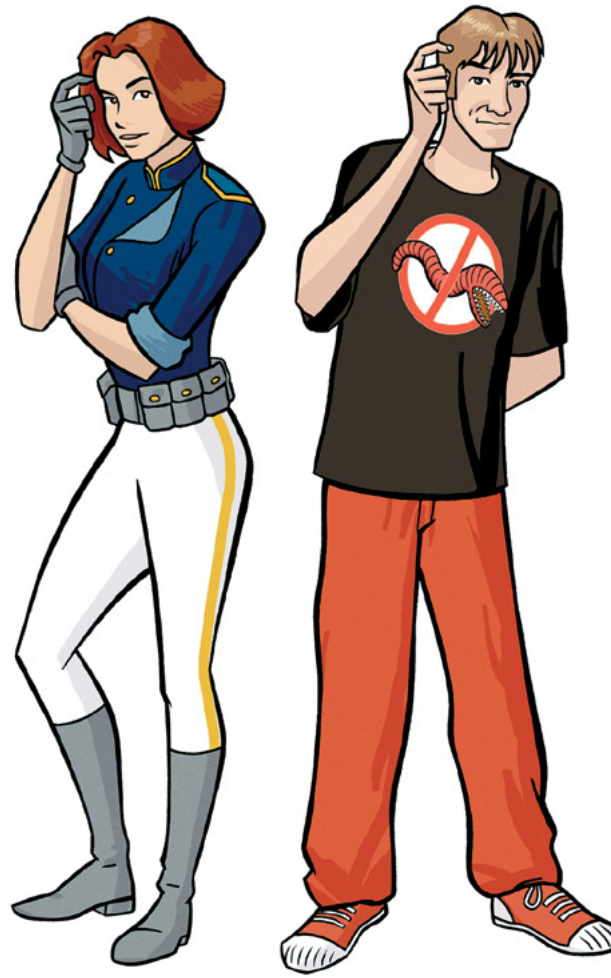
DRUGO IZDANJE

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnije na Internetu



Nacionalno središte za računalnu sigurnost
National Computer Emergency Response Team

Nacionalni CERT

Sadržaj

Impressum

Hrvatska akademska i istraživačka mreža CARNet

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Josipa Marohnića 5, Zagreb
tel: 01 6661 616
fax: 01 6661 615
http://www.CARNet.hr

Nacionalni CERT

Nacionalno središte za računalnu sigurnost
National Computer Emergency Response Team
Nacionalni CERT+

Uvod

Pred vama je knjižica o sigurnijem korištenju računala na Internetu. Ona će vam pomoći boljem razumijevanju opasnosti koje vrebaju u virtualnom svijetu, naučiti vas kako prepoznati prijevare, zaštititi vaše računalo i sačuvati vaše podatke od krađe ili gubitka. Cilj je Nacionalnog CERT-a, odjela CARNeta zaduženog za računalnu sigurnost na Internetu u Republici Hrvatskoj, opremiti vas potrebnim znanjem kako biste sigurnije i s više povjerenja koristili prednosti novih tehnologija.

Razumljivo je da većina današnjih korisnika računala nisu, niti žele, postati računalni stručnjaci. Računala i pametne telefone koristimo za pristup novom mediju weba, za komunikaciju i posao. Uz pomoć uputa koje ćete ovdje pronaći moći ćete se uz manje nepoznanica i opasnosti posvetiti korištenju računala u svrhu koja je vama važna. Brigu o sigurnosti ne možete otkloniti, no možete je učiniti manje neugodnom i nepoznatom.

Dok su u ranijim godinama najveće opasnosti bile koncentrirane u tehničkim propustima softvera koji koristimo, razvojem tog softvera korisnik postaje lakša meta pa svjedočimo porastu pokušaja prijevare u svim zamislivim oblicima. Vaše znanje i kritičko promišljanje osnovna je linija obrane vaše sigurnosti. Kako se naš identitet u moderno vrijeme često sastoji samo od nekolicine podataka u pravim kombinacijama, zaštita naše privatnosti ubrzano se penje na vrh prioriteta pri korištenju novih tehnologija.

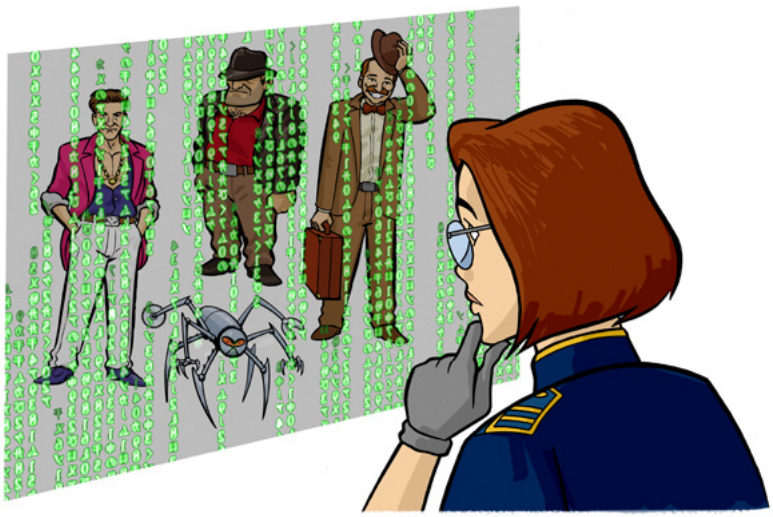
Uz bolje razumijevanje potencijala vaših osobnih podataka i načina na koji moderne usluge funkcioniraju, vaše iskustvo korištenja računala opet može postati ugodno i lišeno straha. Želimo vam ugodno surfanje i dobre valove!

Vaši: CARNet i Nacionalni CERT

Pojam računalne sigurnosti posljednjih se godina sve više prepoznaje i izvan stručnih krugova. Polako uviđamo kako korištenje računala na globalnoj mreži sa sobom nosi niz odgovornosti i sigurnosnih pravila, kao što to vrijedi za upravljanje vozilom ili održavanje plinske instalacije u kućanstvu. Ipak, opasnosti napreduju brže od razvoja svijesti o njima i ne potrudimo li se uhvatiti korak, ostajemo im izloženi.

Ova brošura nastoji vam upravo u tome pomoći, dajući vam znanje potrebno da biste opasnosti prepoznali i izbjegli.

Iza virtualne zavjese

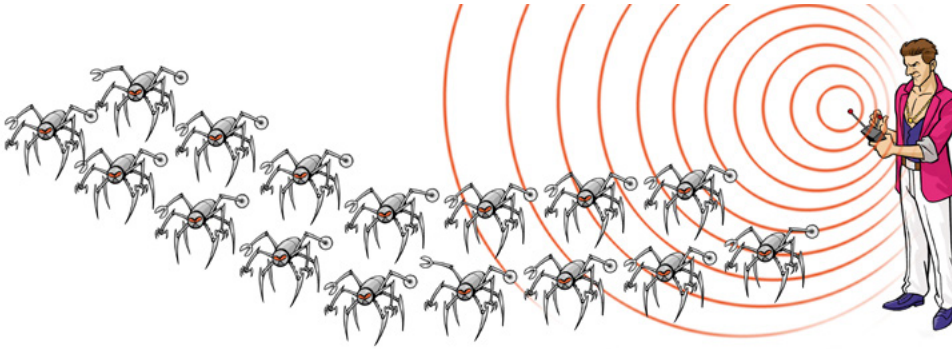


Zašto je uopće globalna mreža u tolikoj mjeri preplavljena opasnim i neželjenim sadržajem? Kome je i zašto u interesu baciti naše kućno računalo na koljena i učiniti ga jedva upotrebljivim?

Važno je razumjeti da je naše računalo, kada ga spojimo na Internet, dostupno svim drugim računalima spojenima na Internet, komunicirali mi s njima ili ne. Internet je mreža u kojoj su svi međusobno povezani. Naše računalo samo po sebi i nije posebno zanimljivo, no tisuće takvih kao što je naše predstavljaju velike resurse s kojima se štošta može napraviti.

U današnje vrijeme, ako je vaše računalo zaraženo, ono vrlo vjerojatno sudjeluje u koordiniranoj mreži sličnih zaraženih računala i svima njima upravlja autor malicioznog kôda koji ste "pokupili". Vaše računalo koristi se za raspačavanje neželjene pošte, razbijanje lozinki, napade na web poslužitelje, daljnje širenje malicioznog kôda i slično.

Centralno upravljanu mrežu sastavljenu od zaraženih računala zovemo **botnet**, a maliciozni kôd na takvim zaraženim računalima **bot**.



No opet se postavlja pitanje: zašto je to nekome u interesu? Ako netko sastavi prijevaru (više o njima u poglavlju o prijevarama) u koju je vrlo teško povjerovati i pošalje vam je, šanse da ćete nasjesti su vrlo male. No ako je pošalje na milijun adresa, već će, nada se, naići netko manje kritičan. Također, ako netko poslužuje ilegalnu web stranicu na jednom poslužitelju, brzo će ostati bez nje. Ako je poslužuje na brojnim kućnim računalima i izmjenjuje adrese, stranica dugo opstaje. Na većem je broju računala također veća vjerojatnost pronalaženja podataka o broju kreditne kartice, lozinki servisa koji upravljaju vašim novcem i slično.

Naravno, postoji još mnogo načina na koje kriminalci mogu zaraditi na vašem zaraženom računalu, o kojima ćete više saznati u nastavku ove brošure.

Putevi do kontrole našeg računala

Kako se zlonamjeran kôd probije do našeg računala i odakle dolazi? Često ustanovimo da s računalom nešto nije u redu, a ne možemo se sjetiti ničeg sumnjivog što bismo s time povezali.

Važno je razumjeti da se zlonamjeran sadržaj može nalaziti i u tipovima datoteka u kojima ga obično ne očekujemo, npr. u dokumentima (**pdf, doc, xls...**), čak i onda kada ti dokumenti izgledaju dobroćudno. Zbog toga je važno sve aplikacije koje

dolaze u kontakt s datotekama preuzetima s Interneta redovito ažurirati, kako bi se na vrijeme primijenile sigurnosne zakrpe njihovih proizvođača.

S obzirom na to da tipičan korisnik najviše vremena provede koristeći web preglednik, ta je aplikacija ujedno i najzanimljivija autorima zlonamjernog kôda. Redovito ažuriran web preglednik teško će dopustiti automatsku ugradnju bilo kakvog kôda bez odobrenja korisnika pa autori uglavnom pribjegavaju manipulaciji korisnika - socijalnom inženjeringu.

Socijalni inženjering je manipuliranje ljudima u svrhu otkrivanja povjerljivih informacija ili pristupa resursima do kojih manipulator sam ne može doći. Manipulator korisnika prijevarom „navuče“ da otkrije povjerljivu informaciju ili za njega obavi neku radnju.

Tipičan primjer ovakve manipulacije je web stranica s nekim zanimljivim video sadržajem, koji, da biste ga pogledali, zahtjeva pokretanje aplikacije, *plugina* ili nekog drugog oblika izvršnog kôda na vašem računalu. U stvarnosti se radi o zlonamjernom kôdu koji se bez vaše pomoći ne bi samostalno mogao izvršiti. Poveznice (linkove) na ovakve sadržaje možete primiti putem elektroničke pošte, izmjenjivanjem poruka u realnom vremenu (*Instant Messaging*, npr. ***Skype***), putem društvenih mreža kao što je ***Facebook***, praćenjem sadržaja na ***Twitteru***, u komentarima blogova i na brojnim drugim mjestima.

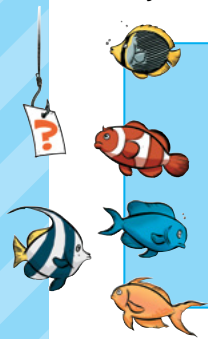
Zlonamjeran kôd može se skrivati i u obliku nekog multimedijalnog sadržaja na P2P mrežama (***BitTorrent*** i slično) - datoteka koja nazivom i veličinom podsjeća na video sadržaj ne mora zaista to i biti. Općenito nije preporučljivo pokretati bilo kakav sadržaj koji ste primili iz nepoznatog izvora, no ako ste se već na to odlučili provjerite je li datoteka zlonamjerna putem besplatnog web servisa **virustotal.com**.

Također, ponekad preuzeta video datoteka sadrži kratak video s uputom da s neke web stranice preuzmete softver za reprodukciju. Takav softver gotovo je redovito zlonamjeran.

Prijevare

Pojam s kojim se sve češće u medijima susrećemo je **krađa identiteta**. S obzirom na to da se danas gotovo sve transakcije u realnom svijetu mogu obaviti predočavanjem određenih osobnih informacija, te su informacije modernim kriminalcima iznimno zanimljive. Kada ih prikupe, mogu u naše ime naručivati proizvode i usluge ili upravljati našim bankovnim računima.

Uobičajen način na koji se te informacije od nas prikupljaju zove se *phishing* (eng. *fishing* - pecanje), a radi se o masovnom zasipanju velikog broja osoba porukama u kojima ih se nastoji nagovoriti da svoje osobne podatke upišu u formular na nekoj web stranici. Logika kojom se vode je da će se valjda netko „upecati".



Phishingom se kradu različiti osobni podaci: korisnička imena i lozinke za pristup servisima kao što su web mail, Facebook ili PayPal, a u opasnijem slučaju PIN-ovi naših kreditnih i debitnih kartica. Tipičan phishing započinje porukom koja izgleda kao da je stigla od banke ili web stranice čije usluge koristimo, u kojoj nam se objašnjava da je zbog sigurnosne provjere potrebno prijaviti se na njihovu web stranicu i upisati svoje podatke. Stranica na koju nas ta poruka odvodi izgledom će imitirati servis koji koristimo, no upisani podaci završit će u rukama prevaranta.

From: Cornell Security <netid@cornell.edu>

Subject: BLACK LISTED ACCOUNT (DO NOT IGNORE)
Date: October 21, 2016

Dear User,

We received a request on 20/10/16 to deactivate your account. Please confirm this request to complete the deactivation process:

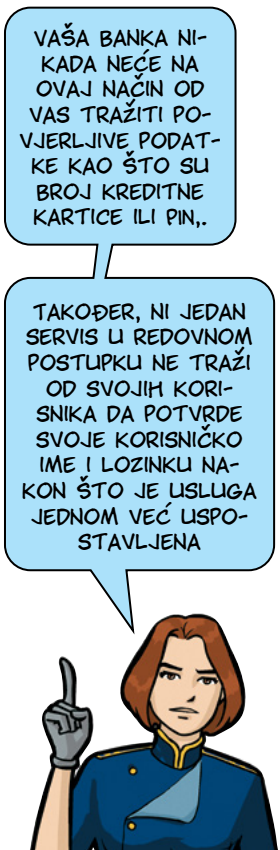
Yes, I would like to deactivate my account

No i didn't make this request, cancel deactivation request

To make additional edits to your account, sign in to www.edit.mail.Cornell.edu

Thank You,
Cornell Account Team

Please do not reply to this message. Mail sent to this address cannot be answered.
© Cornell T INC 2016



Osnovni razlog popularnosti *phishinga* kao metode prikupljanja povjerljivih osobnih podataka je to što se prevaranti ne moraju truditi pronaći propuste u sigurnosnoj zaštiti vašeg računala - korisnik svojevoljno upisuje informacije. Isto vrijedi i za ostale oblike prijevara.

Jeste li kada dobili poruku elektroničke pošte s obavijesti kako ste dobili na lutriji? Možda se poruka pojavila u sklopu neke web stranice koju posjećujete? Na koji god način ovakva poruka stigla do vas, razmislite: ako zvuči predobro da bi bilo istinito, vjerojatno ste u pravu - nije istinito. Lažni dobici na lutriji samo su lukav način da vas se nagovori da uplatite razmjerno malen iznos za "troškove obrade", čime priča o vašem dobitku ujedno i završava. Potpuno jednak princip vrijedi za priče o nasljedstvu prinčeva iz udaljenih zemalja i slične poruke.

Neke od ovih prijevara pokušavaju biti uvjerljivije tako da vam umjesto gotovog novca nude - kredit. Fantastično povoljni krediti iz drugih zemalja,

ponude poslane elektroničkom poštom, sve to trebalo bi u vama pobuditi sumnju, koliko god vam novac u tom trenutku bio potreban. Čak i ako vam se netko obrati na hrvatskom jeziku ili napiše povoljno mišljenje o tom kreditu na nekom forumu, ne nasjedajte!

U novije vrijeme prevaranti će vas čak pokušati nagovoriti da uplatite novac kako biste spriječili objavu nekog neugodnog video zapisa u kojem se navodno pojavljujete (video zapis naravno ne postoji). Neki se moderni crvi služe sličnom metodom (poveznicom na video zapis) kako bi vas pridobili da pristanete na preuzimanje softvera za reprodukciju i tim postupkom zarazite računalo.

Osim ovakvih općenitih prijevara koje se univerzalno koriste, postoje i ciljane prijevare koje se oslanjaju na aktualne događaje. Humanitarna kriza izazvana potresom na Haitiju popraćena je nizom lažnih humanitarnih akcija, pri čemu su ljudi širom svijeta novac uplaćivali lažnim humanitarnim organizacijama. Kako biste izbjegli ovakve prijevare, a ipak ostvarili svoju želju da pomognete, pretražite web i pronađite registrirane humanitarne organizacije čije postojanje i djelatnost možete provjeriti, te za uplate koristite informacije dostupne na njihovim službenim web stranicama.

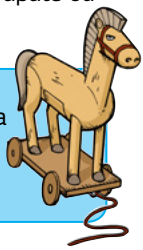
Sve ove prijevare oblici su **socijalnog inženjeringa** jer manipuliraju isključivo ljudima, dok je tehnologija samo sredstvo dosega velikog broja ljudi.

Maliciozan softver (malver)

Do sada smo već spominjali maliciozan kôd, no o čemu se zapravo radi? Popularno zvani virusi ili crvi neki su od brojnih oblika softvera načinjenog s namjerom zloupotrebe računalnih sustava. Kako tih oblika ima sve više, zajedno su okupljeni pod pojmom malicioznog softvera - malvera (eng. *malware - malicious software*).

Malver u praksi razlikujemo po funkciji koju obavlja za svog autora. Neki su oblici potpuno autonomni i izvršavaju unaprijed zadane zadatke (npr. korištenje vašeg računala za raspačavanje neželjene pošte - spama), a neki se nakon ugradnje u računalo pritaje i očekuju upute od svog autora.

Malver koji korisnik sâm ugradi (instalira) u računalo jer se predstavlja kao neki drugi sadržaj (kao u primjeru ranije spomenutog video zapisa) zovemo **trojanskim konjem.**



Osim manipulacijom korisnika, malver se ugrađuje u računalo i korištenjem sigurnosnih propusta softvera koji koristite. To znači da takav malver s jednog zaraženog računala na drugo može putem mreže prijeći bez ikakve interakcije s korisnikom i bez ikakve vidljive reakcije računala, ali pod uvjetom da je ciljno računalo ranjivo.

Zamislite da ste na ulaz u kuću ugradili protuprovalna vrata, no imate prozore koji se daju otvoriti izvana. S vratima je sve u redu, no vaša je kuća svejedno izložena riziku od provale - dovoljno je da provalnik primijeti vaš propust. U slučaju softvera, propusti nestručnim očima uopće nisu vidljivi i moramo se osloniti na proizvođača.

U prvom se redu rizik sigurnosnih propusta odnosi na vaš operativni sustav (npr. ***Microsoft Windows***), zatim web preglednik (npr. ***Mozilla Firefox***), a ponekad i preglednike dokumenata i multimedijalnih datoteka (npr. ***Adobe Acrobat Reader, Windows Media Player***). Proizvođači pronađene sigurnosne propuste u pravilu ispravljaju i korisnicima distribuiraju ažurne inačice, no na nama je da te inačice redovito preuzimamo i pokrećemo.

Jednom ugrađen u naše računalo, malver može pretražiti naše dokumente, elektroničku poštu i zapise o po-

sjećenim stranicama te iz tih izvora saznati povjerljive podatke. Ako mu nedostaje korisničko ime i lozinka za neku uslugu koju koristimo, pričekat će da posjetimo web stranicu gdje te podatke upisujemo te ih preuzeti dok koristimo tipkovnicu ili pronaći u mrežnom prometu između našeg računala i Interneta. Prikupljene će podatke zatim poslati na adresu nekog računala pod kontrolom autora* (često je i to samo računalo zaraženo nekim oblikom malvera), odakle ih on preuzima i dalje koristi.

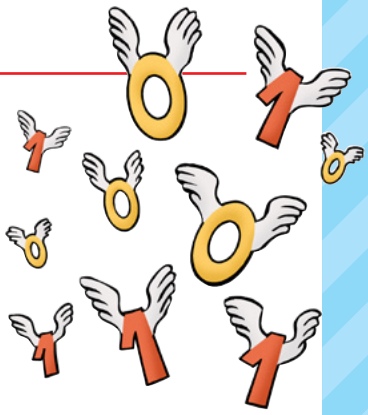
Jedna od posebno opasnih vrsti malvera je tzv. "***ransomware***" koji nakon što inficira računalo, kriptira datoteke (time ih čini neupotrebljivima) i traži otkupninu kako bi vratio naše datoteke. Često su time te datoteke (obično dokumenti) zauvijek izgubljene, čak i ako se otkupnina (u iznosu nekoliko stotina eura pa i više) plati. Plaćanje otkupnine se ne preporučuje jer se time financiraju kriminalne skupine. Jedina efikasna obrana od ove vrste malvera je redovita izrada pričuvnih kopija (v. Pohrana pričuvnih kopija).

Malver s vašim računalom može činiti sve što i vi sami - već smo spomenuli kako vam poruke s opasnim poveznicama mogu doći i od vaših prijatelja putem društvenih mreža. Kada je na vašem računalu malver i vaš će virtualni identitet biti korišten na taj način.

Danas najopasniji malver pritajeno čeka da pristupite web sučelju svoje banke i u standardne formulare ubacuje dodatna polja s podacima koje od vas želi ukrasti (npr. PIN vaše kartice koji banka obično od vas ne traži u sklopu elektroničkog bankarstva). Te podatke također pritajeno prosljeđuje osobi koja malverom upravlja.

*Autor može prodati pristup malverom zaraženim računalima nekoj trećoj osobi i u praksi to najčešće i jest tako.

Bežične mreže



Današnja prijenosna računala standardno dolaze s opremom za povezivanje na bežične mreže. Terminalna oprema koju dobivate kada preuzimate priključak na Internet također uglavnom dolazi s bežičnom pristupnom točkom. Bežične su mreže svuda oko nas i omogućavaju nam veću mobilnost i udobnost. Također, ako nisu ispravno podešene, omogućavaju svakome u našoj blizini da se u njih uključi, prisluškuje i pristupa Internetu koristeći naš priključak.

Ako koristimo samo jedno stolno računalo u kući, lako se zaštititi od bežičnih opasnosti - jednostavno spojimo računalo na uređaj za pristup Internetu koristeći običan mrežni kabel te isključimo bežični primopredajnik na pristupnom uređaju i na računalu. Upute za isključenje bežičnog primopredajnika dobivamo s uređajem, a ako smo ih izgubili možemo se savjetovati s korisničkom podrškom.

Ako nam je bežična mreža potrebna, prvo trebamo osigurati ispravnu kontrolu pristupa i enkripciju informacija koje se radio valovima šire kada računalo komunicira s pristupnom točkom. Većina pristupnih uređaja i računala nudi WEP, WPA i WPA2 standarde enkripcije te korištenje kraćeg ili dužeg ključa za kontrolu pristupa.

WPA i WPA2 su dobri standardi enkripcije i uz nasumičan ključ čine odgovarajuću zaštitu vaše mreže. Svakako koristite potpuno nasumičan ključ - bez riječi, imena, datuma ili bilo čega drugog smislenog. Računalo će pohraniti vaš ključ i više vas za njega neće pitati te nema potrebe da bude lako pamtljiv.

Koristimo li tuđe pristupne točke, potrebno je obratiti pažnju na dvije stvari:

1. Radi li se o nezaštićenoj (nekriptiranoj ili WEP kriptiranoj) mreži?
2. Znamo li kome mreža pripada i možemo li mu vjerovati?

Kada pristupamo nezaštićenoj bežičnoj mreži, sva računala u dometu mogu "preslušavati" informacije koje naše računalo odašilje i prima. Na ovaj način mogu se ukrasti lozinke i drugi važni podaci, a u nekim slučajevima moguće je pristupiti i sadržaju tvrdog diska vašeg računala. Ako je vaše računalo pri tom još i ranjivo (više o ranjivostima u idućem poglavlju), moguće je potpuno preuzimanje kontrole bez vašeg znanja.

Pristupamo li bežičnoj mreži čijeg vlasnika ne poznajemo, izlažemo se istom riziku kao i u slučaju nezaštićene mreže: tko god kontrolira pristupnu točku, može steći pristup našem računalu.

Kako se zaštititi

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

Na tehničkoj razini, računalo je potrebno zaštititi odgovarajućim sigurnosnim softverom te ispravnim podešenjima operativnog sustava i aplikacija. Srećom, danas postoji mnoštvo kvalitetnih besplatnih rješenja na ovom području. Izdvojit ćemo najvažnije elemente zaštite i pravila kojih se dobro držati.

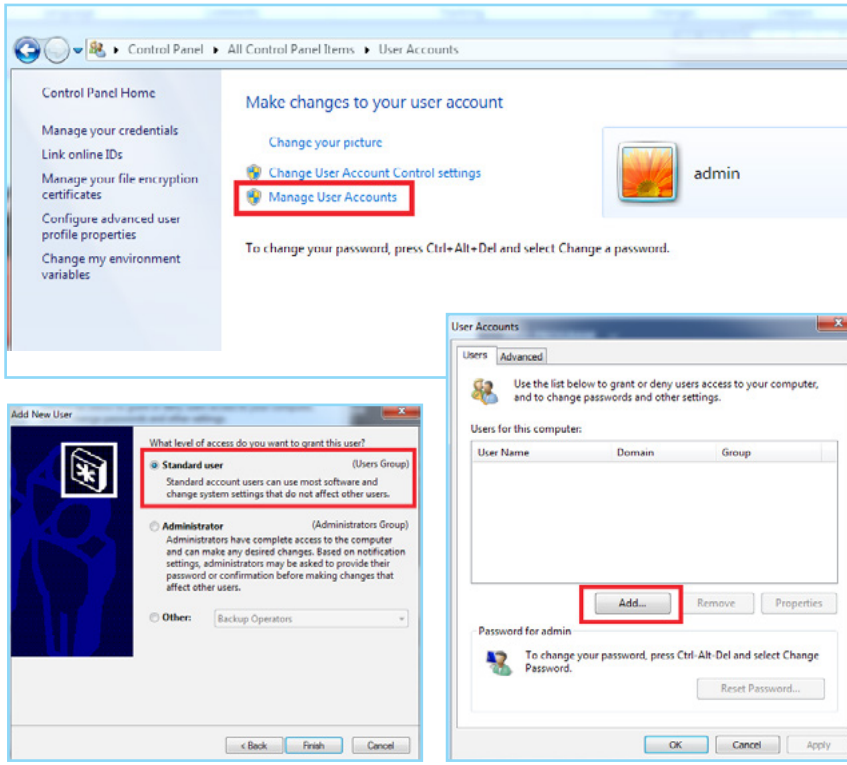
01 Antivirus/antispyware/antimalware - rješenja za prepoznavanje i zaustavljanje aktivnosti malvera. Antivirusni alat je obavezan dio softverske opreme vašeg računala. Neka rješenja dolaze u paketima sa drugim sigurnosnim softverom (npr. vatrozidom), dok su neka samostalna. Operacijski sustav ***Windows*** 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.

02 Vatrozid - aplikacija koja ograničava mrežnu komunikaciju između vašeg računala i Interneta; selektivnim propuštanjem prometa izbjegava se neovlaštena komunikacija i smanjuje mogućnost iskorištenja sigurnosnih propusta u aplikacijama koje ne koristite, a koje imaju mogućnost mrežne komunikacije. Windows operativni sustav (XP i noviji) po ugradnji u računalo već sadrži vatrozid s odgovarajućom zaštitom.

Vatrozid će vas upitati za odobrenje svaki puta kada neka nova aplikacija pokuša poslati podatke putem mreže.

03 Automatsko ažuriranje operativnog sustava i aplikacija - sigurnosni propusti u softveru stalno se otkrivaju. Kako vas ne bi ostavili ranjivima, uključite automatsko ažuriranje u operativnom sustavu i svim aplikacijama koje dolaze u kontakt sa sadržajima s Interneta (npr. čitači za PDF dokumente). Operacijski sustav ***Windows*** promatra je li automatsko ažuriranje operativnog sustava uključeno te upozorava korisnika ako nije.

04 Korištenje korisničkog računa sa smanjenim privilegijama (*Standard user*) - preporučljivo je da korisničko ime kojim se služite u svakodnevnom radu ima ograničen pristup računalu. Na taj način, većina malvera jednostavno neće imati pristup ključnim dijelovima operativnog sustava 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 imenom.



05 Alternativni softver - autori malvera ciljaju softver s najvećom bazom korisnika. Ako je moguće, koristite alternativne klijentske aplikacije i preglednike; to se odnosi na web preglednik, klijent elektroničke pošte, preglednik PDF dokumenata, softver za reprodukciju multimedije i sve što dolazi u kontakt sa sadržajem s Interneta. Možete koristiti čak i alternativni operativni sustav, kao što je ***Ubuntu Linux***.

06 Provjereni sigurnosni alati - kada odabirete sigurnosne alate, ne nasjedajte na oglase po sumnjivim web stranicama. Često se malver krije u obliku lažnog antivirusnog softvera ili stranice koja imitira da je na vašem računalu upravo pronađen virus! Kako biste bili sigurni da koristite provjeren softver, potražite sigurnosni alat koji vas zanima na stranicama Nacionalnog CERT-a ili na portalu AntiBot:

- http://www.cert.hr/alati
- http://www.antibot.hr

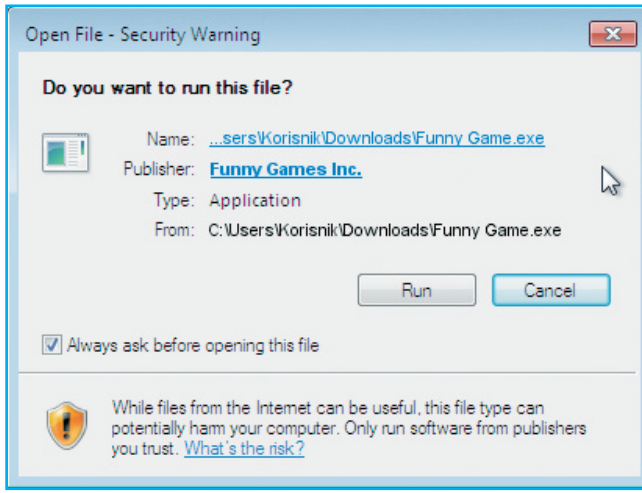
Upravljači lozinkama (password managers) vaše lozinke kriptiraju i štite jednom glavnom lozinkom - master password. **Apsolutno je nužno da ta lozinka bude što složenija i da slijedi pravila opisana u ovoj točki.** Većina softvera za upravljanje lozinkama testira kompleksnost vaše glavne lozinke pri upisu.

07 Složene i različite lozinke - računala iznimno brzo mogu isprobavati različite kombinacije imena i lozinki pa su lozinke koje sadrže riječi iz govornog jezika, datume, imena i slično iznimno jednostavne za pogađanje. Dobra lozinka sastoji se od 10 znakova, mješavine slova i brojki. Dodatnu sigurnost pruža korištenje velikih i malih slova te interpunkcijskih znakova. Razumljivo, ovakve je lozinke teško upamtiti, pogotovo ako su različite za svaki servis. Zato postoje aplikacije za upravljanje lozinkama (eng. password manager) koje pomoću jedne lozinke štite sve ostale. Jedna takva aplikacija je ***KeePass Password Safe***.

Windows 7 pri izvršavanju kôda kojem je potreban pristup zaštićenim dijelovima operativnog sustava zatamni ekran i pita korisnika za dopuštenje. Ako niste sami pokrenuli ugradnju aplikacije za koju pouzdano znate što radi, ne odobravajte ovu akciju!

Kako prepoznati opasnost

Kako bismo spriječili izvršavanje stranog kôda na svojem računalu, prvo moramo znati prepoznati situacije u kojima nas računalo pita za dozvolu da se neki kôd izvrši. Naš će nas web preglednik i operativni sustav upozoriti u svakoj situaciji u kojoj se datoteke preuzete s Interneta trebaju izvršiti i dati nam priliku da to odbijemo.

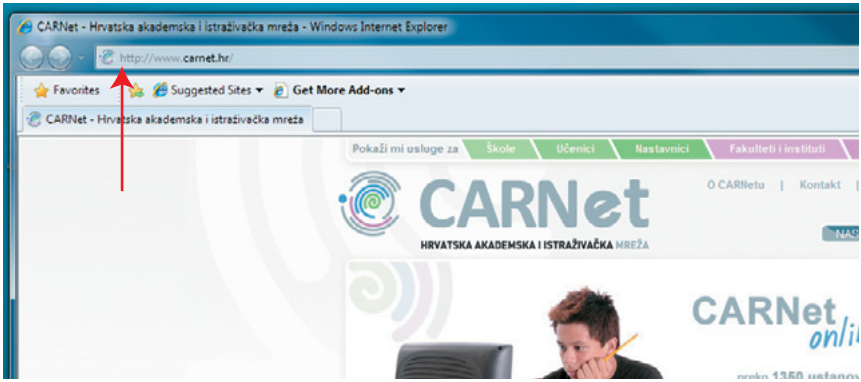


Kako znati trebamo li dopustiti izvršenje ili ne? Radi li se o iznenadnom upitu, odgovor je zasigurno ne; dozvolu za izvršavanje trebamo dati isključivo aplikacijama koje smo željeli pokrenuti.

Na računalo nije mudro ugrađivati svaku aplikaciju koja nam se učini zanimljivom niti odobravati ugradnju komponenti za koje nismo sigurni čemu služe. Mnogo je sigurnije nove aplikacije tražiti u sklopu servisa koji provjeravaju o kakvom se softveru radi, kao što je web stranica **download.com**. Radi li se o sigurnosnom alatu, provjerite pojavljuje li se taj alat na stranicama Nacionalnog CERT-a i koristite priložene poveznice: ▶ http://www.cert.hr/alati

Kod nekih web stranica postoji veća vjerojatnost da ćemo zateći maliciozan kôd koji već prilikom prikaza stranice pokušava iskoristiti propuste u našem web pregledniku ili nas prevariti. Takav se kôd 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.

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 poveznicu 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 poveznica 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 naše računalo zaraženo ako se to ipak dogodi? Malver se često stvara brže nego što to proizvođači antivirusnih alata mogu pratiti pa vaše računalo može biti zaraženo, a da to antivirus ne može prepoznati.

Na žalost, nema jamstva da će zaraženost biti moguće ustanoviti, no neki nam pokazatelji ipak mogu odati prisutnost malvera. Pojavljuju li se na računalu spontano alarmantni upiti, kao što je prozor s upozorenjem da će se računalo 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, vaše računalo je gotovo sigurno zaraženo.

Elektronička trgovina

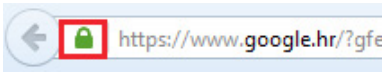
Internet nam omogućuje kupovinu robe i usluga iz udobnosti našeg doma, uz korištenje naše kreditne kartice. Jasno je da vaše ime, adresa i brojevi na kartici čine dobitnu kombinaciju za korištenje vaših sredstava. Stoga je od presudne važnosti da ti podaci s vašeg računala ne "procure".

Neki servisi za plaćanje nakon jednog korištenja pamte podatke o vašoj kartici i iduća kupovina moguća je uz korištenje samo korisničkog imena i lozinke. U tom slučaju, smatrajte korisničko ime i lozinku jednako osjetljivim podatkom kao i sve informacije o vašoj kartici. Ako je moguće, preporučujemo uklanjanje podataka o kreditnoj kartici iz web profila nakon korištenja.

Malver je posebno zainteresiran za krađu podataka o vašoj kreditnoj kartici pa je važno da se karticom koristite na računalu koje je izloženo što manjem riziku: dakle računalu na kojem ne pristupate rizičnim web stranicama te ne preuzimate i ne pokrećete sadržaje s Interneta. Slično tome, elektroničku kupovinu nije preporučljivo obavljati na neprovjerenim javnim računalima. Na računalu u web kafiću ili sličnom mjestu može biti prisutan malver.

Kako prepoznati web stranice na kojima je sigurno kupovati? Kradljivci kreditnih kartica žele ostati neotkriveni i zato koriste web stranice čije vlasnike nije moguće provjeriti. Ako web stranica koristi HTTPS protokol i posjeduje ispravan certifikat o vlasniku te stranice, identitet vlasnika je provjerljiv i prevaranti mu nisu skloni.

Što je HTTPS i što čini ispravan certifikat? Svaka web stranica koju učitamo u web preglednik na početku svoje adrese u adresnoj traci sadrži oznaku protokola (obično "http://"). Kada web stranica koristi HTTPS protokol, početak adrese glasi "https://". Također, web preglednik će bojom ukazati na korištenje sigurnog protokola i ispravan certifikat.



Mozilla Firefox

Microsoft Internet Explorer

Google Chrome

Elektroničko je bankarstvo daleko najosjetljivija kategorija elektroničkog poslovanja. Danas većina banaka nudi dobar sigurnosni sustav s uređajima za jednokratne zaporke (*token*), pametnom karticom (*smartcard*) ili sličnom tehnologijom koja onemogućava višekratni pristup istom lozinkom ili ključem. To čini vaše pristupne podatke manje osjetljivima na krađu.

Tijela ovlaštena za izdavanje certifikata zovu se *CA - Certificate Authority*. Naš web preglednik prihvatit će samo certifikate izdane od organizacija koje su za to ovlaštene i priznate. Neki od poznatih CA-ova su **Thawte** i **Verisign**.

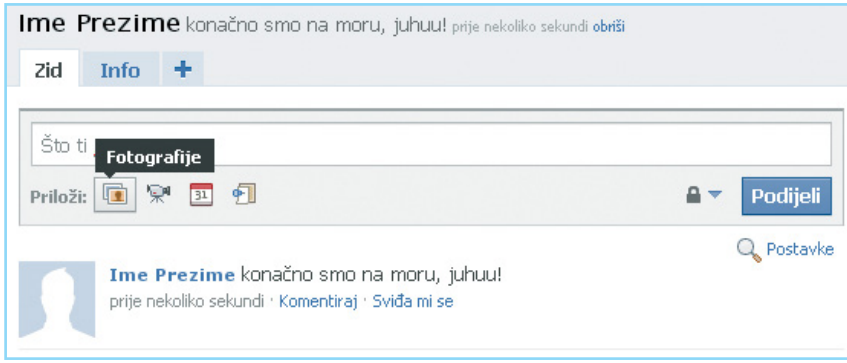
Zbog ovakve zaštite, kriminalci pribjegavaju sofisticiranijim metodama, kao što je umetanje unosnog polja (PIN) u web stranicu banke prilikom prikazivanja u web pregledniku (vidi: Malver) ili socijalnom inženjeringu (vidi: Prijevare).

Osim načina pristupa, za elektroničko bankarstvo apsolutno je nužna prisutnost HTTPS protokola i ispravnog certifikata. Ne propustite provjeriti je li vaš web preglednik ispravno prepoznao HTTPS protokol i pripadajući certifikat na ovdje opisan način.

Privatnost

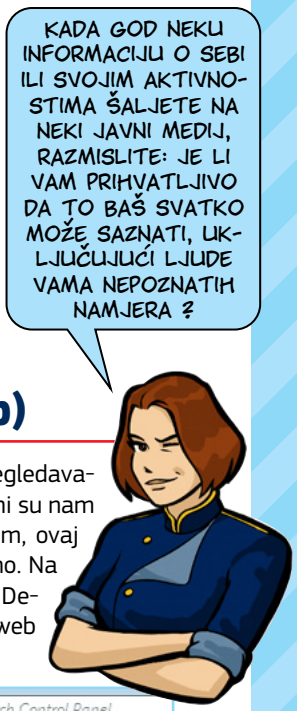
Do sada smo uglavnom govorili o zaštiti podataka koje je moguće neposredno zloupotrijebiti, kao što su podaci o našim karticama ili naše lozinke. No podaci o nama samima nisu ništa manje važni i dobro je razmisliti prije nego što neku informaciju o sebi ili svojim aktivnostima podijelimo sa cijelim svijetom.

Što to može biti opasno u privatnim informacijama o nama? Najjednostavniji primjer je svakako informacija da niste kod kuće u neko točno određeno vrijeme, a ako je uz to poznato i gdje živite, to je kao da ste objavili reklamu za pljačku svog doma. Osim toga, dovoljno detaljne informacije o vama drugima daju mogućnost da se lažno predstavljaju kao vi i tako koriste usluge koje ste platili ili prevare nekog vama bliskog.



Danas najviše informacija sa svijetom dijelimo putem društvenih mreža (npr. ***Facebook***) i *microblogging* servisa kao što je ***Twitter***. Te su aktivnosti postale toliko uobičajen način komunikacije da ponekad zaboravimo koliko je širok krug ljudi koji sve to vide, a uz to nam najveći operateri društvenih mreža ne garantiraju da jednog dana podaci koji su bili vidljivi samo našim prijateljima neće postati javni.

Kada govorimo o privatnosti, uređaj na kojem često držimo pohranjene iznimno osjetljive informacije je i naš mobilni telefon. Kada ugrađujemo neku igru ili aplikaciju, taj softver svim tim osjetljivim informacijama ima pristup, a kao i mogućnost da u naše ime šalje poruke i upućuje pozive na visokotarifne brojeve. Imate li u mobilnom telefonu zapisane PIN-ove ili lozinke, zlonamjerna aplikacija i do njih može doći. Zato je važno aplikacije preuzimati isključivo preko distributera kojima vjerujemo i za koje znamo da provjeravaju sadržaj i funkcionalnost ponuđenih proizvoda.



Pohrana pričuvnih kopija (backup)

Koristimo li računalo za išta ozbiljnije od povremenog igranja i pregledavanja sadržaja na Internetu, podaci koje na njega pohranjujemo važni su nam i postanu li nedostupni to može predstavljati veliku štetu. Srećom, ovaj je problem danas značajno lakše rješiv nego što je bio još nedavno. Na raspolaganju su nam brojne jeftine ili čak besplatne mogućnosti. Detaljne upute koristeći jedno od besplatnih rješenja nalaze se na web stranici http://www.cert.hr/ransomware

Najjednostavnije je kritične podatke povremeno kopirati na vanjski medij, kao što je prenosiva memorija ili optički disk (CD, DVD, HD-DVD, Blueray), uz napomenu da redovito kopiranje od nas zahtjeva određenu dozu discipline. Važno je da medij na koji pohranjujemo pričuvne kopije nije stalno priključen na računalo s kojeg podaci dolaze, jer se na taj način original i kopija izlažu nekim zajedničkim rizicima, kao što je rizik od električnog udara i ransomware-a.

Druga raširena mogućnost je pohrana pričuvnih kopija na za to specijaliziranim Internet servisima uz koje dolazi softver za upravljanje procesom izrade pričuvnih kopija. To je vrlo praktično rješenje, no postoje rizici:

- tvrtka koja upravlja našim kopijama može izgubiti naše podatke, stoga ih ne možemo povjeriti bilo kome
- tvrtka može propasti
- softver koji naše podatke šalje na pohranu može ih slati bez enkripcije i tako kompromitirati
- u slučaju da softver sam upravlja enkripcijom, tvrtka koja drži naše podatke može im i pristupati bez našeg znanja

Dobra usluga udaljene pohrane naših podataka morala bi zadovoljavati sljedeće kriterije:

1. Enkripcija pod kontrolom korisnika: samo korisnik ima ključ koji može dekriptirati podatke*
2. Iz više smo neovisnih izvora potvrdili ugled i stabilnost tvrtke kojoj povjeravamo naše podatke
3. Uvjeti korištenja servisa te garancija dostupnosti su nam razumljivi i prihvatljivi.

Naposljetku, treba se osigurati od situacije gdje smo napravili neželjenu izmjenu nekog dokumenta i takvu izmjenu pohranili u pričuvnu kopiju , a da to nismo primijetili. Zbog toga je za dokumente i druge datoteke koje mijenjamo mudro kreirati arhivske kopije drugog imena kako bismo spriječili prepisivanje.

*Kriteriju 1. možemo doskočiti na način da podatke koje pohranjujemo pomoću ovakvog servisa prethodno sami kriptiramo koristeći se alatom za enkripciju na vlastitom računalu. Na ovaj način proširujemo izbor ponuđača i možemo pronaći jeftinije rješenje. Na web stranicama Nacionalnog CERT-a možete pronaći neke takve alate.

Vodič za roditelje

Možda ste kao roditelj navikli znati više od svog djeteta o stvarima s kojima se ono prvi put susreće u životu. Računala su jedan od primjera gdje gotovo sigurno nije tako. Čak i ako su računala 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.

Nove tehnologije i mediji neizbježni su i dostupni na mnogo mjesta izvan vašeg doma, čak i s mobilnih telefona. Ne zavaravajte se da im možete efikasno ograničiti pristup. Želite li vašem djetetu pružiti sigurnost u ovom novom prostoru, morat ćete ga i sami dobro upoznati. Ovaj je prostor preuzak da bismo vas naučili detaljima korištenja svih ovih tehnologija. Savjetujemo vam da se na društvene mreže i druge servise koje spominjemo i sami uključite i pokušate njima služiti - nije toliko teško koliko se na početku čini, ipak su ti servisi napravljeni pristupačnima kako bi zainteresirali što veći broj korisnika.

Dok odrasli društvene mreže uglavnom koriste za održavanje kontakata s poznatim ljudima, djeci su one često puno značajnije te su bitan dio njihovog društvenog života. Bit će sklona nesvjesno otkriti vrlo privatne detalje o sebi i svojoj obitelji, postaviti fotografije ne razmišljajući tko ih sve može vidjeti, a ako su osjetljivija, lako će postati metom zadirkivanja svojih vršnjaka na vrlo javan i za njih bolan način.

Razgovarajte o korištenju društvenih mreža i osvijestite rizike svom djetetu - podsjetite ga da sve što jednom objavi o sebi više ne može povući te da postavljanjem svojih i tuđih fotografija odnosno videozapisa može svoje vršnjake, a i sebe, dovesti u neprilike.

Znajte da društvene mreže ne mogu efikasno provjeravati identitete svojih korisnika pa je lako moguće da dijete od vaših restrikcija pobjegne na drugu mrežu ili jednostavno otvori drugi profil. Društvene su mreže sve brojnije i teško ćete pratiti gdje je sve vaše dijete virtualno prisutno. Nastojte izgraditi povjerenje i izbjegnite igru mačke i miša u kojoj ne možete pobijediti.

Osim društvenih mreža za koje vjerojatno znate, a možda ih i sami koristite, vaše dijete može otvoriti blog ili imati profil na **Twitteru** te tako biti virtualno prisutno. Možda nećete moći postići da na **Facebooku** ne koristi svoje pravo ime (iako bi to bilo poželjno), no to mu svakako savjetujte za ove druge medije.

U poglavlju **Kako se zaštititi** pronaći ćete upute o dobrim lozinkama - pobrinite se da i vaše dijete koristi dobre lozinke kako biste spriječili zlouporabu njegovih profila.

Kako bi ta anonimnost imala smisla, na profilu na **Facebooku** ne bi trebalo biti poveznice (linka) na njihov anonimni blog ili profil na **Twitteru**.

Do sada spomenute tehnologije ostavljaju barem nekakav trag nakon korištenja. S druge strane, razne stranice i programi za čavrljanje (chat) često ne ostavljaju nikakav zapis o tekstovima i drugim sadržajima koji su kroz njih prošli. Ne znaju li vaša djeca unaprijed što mogu očekivati, lako mogu postati žrtvama nekoga tko se lažno predstavlja i čije namjere nisu bezazlene.

Čavrljanje dolazi u najrazličitijim oblicima. Društvene mreže (kao **Facebook**) imaju ugrađenu mogućnost čavrljanja. Programi za trenutnu komunikaciju na mobilnim uređajima (**Whatsapp, Viber** i **Facebook Messenger**) često služe kao mediji za vrlo delikatne razgovore među vršnjacima, ali i nekome tko se pretvara da je prijatelj vašem djetetu. Razne web stranice nude čavrljanje podijeljeno u interesne grupe ili "sobe" u kojima više sudionika zajedno komunicira.

Izričito spomenite vašem djetetu mogućnost da ga netko pozove na sastanak uživo i upozorite ga kakvoj se opasnosti time izlaže. Istaknite da je vrlo važno strancima s kojima čavrlja ne odavati informacije po kojima bi ga oni mogli pronaći te da izbjegava takva povezivanja.

U anonimnijem obliku, postoje web stranice koje organiziraju takozvane "sobe" za čavrljanje u kojima istovremeno sudjeluje više sugovornika. Ova su mjesta popularna među djecom zbog mogućnosti eksperimentiranja s izmišljenim identitetima i načinom komunikacije koji nije društveno prihvaćen. Poseban oblik stranica za čavrljanje nudi video-komunikaciju s nasumično odabranim sugovornikom. Iako većina ovakvih servisa eksplicitno zabranjuje takve aktivnosti, to nije moguće kontrolirati u zadovoljavajućoj mjeri.

Imate li web kameru ili mobilni telefon s ugrađenom kamerom, kontrolirajte korištenje tih uređaja kako biste zaštitili privatnost vašeg djeteta.

Na nekim web stranicama nalaze se igre iza kojih stoje zlonamjerni autori te će na razne načine pokušati izvući novac. Jedan od načina je da se nastavak igranja uvjetuje upisivanjem podataka o kreditnoj kartici, koju vaše dijete naravno nema.

Naposljetku, web je nepresušan izvor informacija o svemu što bi vaše znatiželjno dijete moglo zanimati i ono će vrlo vjerojatno upravo tamo tražiti odgovore na mnoga svoja pitanja. Kao i svaki drugi medij, web pored točnih i korisnih nudi mnoge informacije upitne kvalitete i sadržaje koji djeci nisu primjereni. Važno je da ste otvoreni i spremni na razgovor o pitanjima koja zanimaju vašu djecu te da osvijestite važnost kritičkog prosuđivanja o sadržajima na koje nailaze.

Do neke je mjere ovakve sadržaje moguće filtrirati kategorijom programa pod zajedničkim nazivom **Parental Control**, a koji u komercijalnim oblicima često dolaze u kombinaciji s antivirusnim i drugim sigurnosnim softverom. Ipak, europske institucije savjetuju roditeljima da prvenstveno razgovaraju s djecom o svemu na što nailaze na Internetu te da računala drže u zajedničkoj prostoriji gdje nad njihovim korištenjem mogu provoditi nadzor. Povjerenje je ovdje nezamjenjivo, jer je pristup ovim medijima dovoljno raširen pa je stoga gotovo nemoguće uspostaviti potpunu kontrolu.

Iako se može činiti zastrašujućim na koliko načina nove tehnologije donose opasnosti, zapravo se radi o samo još jednoj prometnici koju vaše dijete svaki dan mora prijeći. Poznajete li tu prometnicu dovoljno dobro i naučite li ga osnovnoj predostrožnosti, već ste učinili mnogo za njegovu sigurnost.

Ukratko, struka preporučuje držati se sljedećih pravila: educirajte se o servisima koje vaše dijete koristi; postavite pravila korištenja računala; smjestite računalo 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 internetskim prijateljima vašeg djeteta; objasnite važnost privatnosti i anonimnosti; pratite aktivnosti djeteta na društvenim mrežama; koristite softver za roditeljski nadzor (***Parental Control***); osvijestite posljedice postavljanja fotografskog i video sadržaja na Internet.

Zlatna pravila sigurnosti

Detalje svake opasnosti koja nam prijeti na Internetu nije lako upamtiti. Zato smo vam pripremili ovaj brzi podsjetnik o osnovnim koracima koji vas mogu učiniti sigurnijima u svakodnevnom korištenju računala. Želite li bolje razumjeti neko od ovih pravila, uvijek se možete vratiti na prethodna poglavlja na koja se ovdje upućuje.

01 Redovito ažurirajte operativni sustav i sve aplikacije koje dolaze u kontakt sa sadržajima s Interneta (vidi: Kako se zaštititi)

02 Koristite dobru enkripciju na kućnoj bežičnoj mreži i javne bežične mreže kojima vjerujete (vidi: Bežične mreže)

03 Koristite kompleksne lozinke za pristup javnim servisima (društvenim mrežama, elektroničkoj pošti i sl.) (vidi: Kako se zaštititi)

04 Poslujete li s karticama ili koristite servise koji u vaše ime mogu obavljati transakcije, provjeravajte ispravnost certifikata (vidi: Kako se zaštititi)

05 Sve novčane transakcije, a posebno rad s elektroničkim bankarstvom, obavljajte s računala koje je najmanje izloženo riziku zaraze (vidi: Kako se zaštititi)

06 Uvijek sami u web preglednik upisujte adresu web stranice na kojoj poslujete novcem, ne koristite poveznice iz primljenih poruka (vidi: Kako prepoznati opasnost)

07 Kada primite poruku u kojoj vam se nudi ili se od vas traži nešto neočekivano, provjerite radi li se o prijevari (vidi: Prijevare)

08 Čuvajte pričuvne kopije najvažnijih podataka i pri povratu pričuvne kopije provjerite sadržaj antivirusnim alatom (vidi: Pohrana pričuvnih kopija)

09 Ne ugrađujte u računalo aplikacije iz nepoznatih i neprovjerenih izvora, posebno ako se radi o sigurnosnim alatima (vidi: Kako se zaštititi)

10 Ne isključujte vatrozid i antivirusni alat i ne ignorirajte njihova upozorenja (vidi: Kako se zaštititi)

Pojmovi

antivirus - softver za automatsko prepoznavanje i blokiranje zlonamjernog softvera
backup - praksa izrade i održavanja pričuvnih kopija važnih podataka s našeg računala
bot - vrsta malvera specijaliziranog za izvršavanje zadataka primljenih s udaljene lokacije
botnet - koordinirana mreža računala zaraženih botovima
CA - Certificate Authority - tijelo ovlašteno za izdavanje certifikata (vidi str. 19)
certifikat - kriptografski dokument kojim se garantira identitet računala s kojim komuniciramo (vidi str. 19)
društvene mreže - web aplikacije kojima je osnovna namjena povezivanje korisnika po njihovim navikama i/ili interesima (npr. Facebook)
hoax - lažna informacija koja se lančano širi (najčešće lančanim slanjem elektroničke pošte), npr. lažna upozorenja o virusima
HTTPS - protokol za razmjenu web sadržaja između preglednika i poslužitelja koji osigurava autentičnost, povjerljivost i neporecivost tim putem razmijenjenih podataka
limited user account - korisnički račun ili profil korisnika s ograničenim pristupom operativnom sustavu (vidi str. 15)
malver - zajednički naziv za sav softver zlonamjerne namjene (vidi str. 10)
microblogging - objavljivanje kratkih (često duljine jedne SMS poruke) sadržaja na javnom servisu koji svi mogu pratiti (npr. Twitter)
password manager - softver za sigurnije upravljanje lozinkama
phishing - masovno zasipanje velikog broja osoba porukama u kojima se na prijevaru traži odavanje tajnih podataka (vidi str. 7)
P2P mreža - Peer-to-peer mrežnu arhitekturu je moguće zamisliti kao skup računala koji su istovremeno i poslužitelji i klijenti, tj. svako računalo može istovremeno primati i davati resurse (datoteke u slučaju BitTorrenta) drugim sudionicima mreže.
ransomware - vrsta zloćudnoga softvera (malvera) koja korisniku uskraćuje pristup računalnim resursima i traži plaćanje otkupnine za uklanjanje ograničenja. Često šifrira datoteke, kako bi one postale neupotrebljive bez odgovarajućeg ključa za dešifriranje kojeg je potrebno platiti.
scam - ozbiljniji oblik hoaxa, često s ozbiljnim financijskim, pravnim ili drugim posljedicama za žrtvu, npr. pranje ukradenog novca preko računa žrtve
socijalni inženjering - manipuliranje ljudima u svrhu otkrivanja povjerljivih informacija ili pristupa resursima do kojih manipulator sam ne može doći (vidi str. 6)
trojanski konj - malver koji se lažno predstavlja kao korisniku zanimljiv sadržaj kako bi mu korisnik dozvolio izvršavanje
URL - naziv za puni oblik adrese nekog sadržaja na webu, npr. http
vatrozid - softver koji omogućuje selektivnu komunikaciju računala s drugim računalima i internetom, namijenjen blokiranju neželjene komunikacije
WEP - zastarjeli standard za kriptiranje podataka u bežičnim mrežama
WLAN - Wireless LAN - naziv za bežičnu lokalnu mrežu
WPA/WPA2 - aktualan standard za kriptiranje podataka u bežičnim mrežama