Preporuke za sigurnost korisnika Internet bankarstva

Sažetak

Samoborska banka ne šalje klijentima banke e-mail poruke sa privicima (attachment) i vezama (linkovima) na web stranice, niti ne zove klijente preko telefona sa ciljem prikupljanja osobnim podataka, lozinki, te ne navodi klijente banke na instalaciju programa na računalo. Ako dobijete takvu e-mail poruku ili telefonski poziv, ne odgovarajte na pitanja niti ne odajte svoje osobne podatke ili lozinke, te takav slučaj prijavite banci.

S ciljem sigurnosti korištenja računala i usluge Internet bankarstva, preporuka je biti oprezan kod otvaranja e-mail poruka od nepoznatih korisnika, pa čak i od prijatelja ako se u mail poruci traži otvaranje neke Internet veze (linka) ili ako poruka sadrži privitak koji ne očekujete od navedenog prijatelja. Uvijek je potrebno pažljivo pročitati poruku i razmisliti je li ta poruka očekivana i logična u nekom trenutku, jer napadači iskorištavaju osnovne situacije kad su ljudi neoprezni, tj. znatiželju, suosjećanje, strah ili stres.

Napadači će se često pokušati predstaviti (putem e-maila, telefona, SMS-a) kao vaše poznate osobe, kao autoritativne osobe (iz policije, porezne uprave, banke, Microsofta i slično) i tražiti osobne podatke ili lozinke ili vas pokušati nagovoriti na instalaciju nekog programa.

Ako vas vaše računalo ili Internet preglednik (browser) ili Office aplikacija upozorava na nesigurnu Internet vezu (link), nesiguran certifikat ili dokument, ne otvarajte takve stvari, već pročitajte upozorenje i ako niste sigurni, tražite savjet od iskusnih korisnika ili npr. potražite informaciju na https://www.carnet.hr/sigurnost ili na http://www.sigurnostnainternetu.hr/

Za sigurnost računala, preporuka je koristiti najnovije operativne sustave, redovno instalirati sigurnosne nadogradnje za operativne sustave i sve aplikacije koje se koriste na računalu, imati uvijek uključenu aktualnu antivirusnu zaštitu, vatrozid (firewall) te koristiti računalo sa minimalnim ovlastima, tj. kao običan korisnik a ne korisnik sa administrativnim pravima. Za prijavu na računalo i za sve servise na Internetu, obavezno je koristiti lozinke minimalne duljine 12 znakova ili više, te NE KORISTITI identičnu lozinku na svim mjestima.

Posebnu pažnju treba obratiti na korištenje najnovijih verzija Internet preglednika (browser), Acrobat Readera, Flasha i JAVA sa svim sigurnosnim nadogradnjama. Ako vam za korištenje Interneta ili obavljanje posla nisu potrebni Flash ili JAVA, preporuka ih je ukloniti ili onemogućiti sa računala.

Sigurnost računala i Internet bankarstva

Danas pomoću računala i zahvaljujući internetu možemo obaviti mnoštvo zadataka za koje nam je nekada trebalo više vremena i fizički odlazak na lice mjesta. Zahvaljujući internetu možemo slati e-poštu, razmjenjivati poruke u stvarnom vremenu (*instant messaging, chat*), zabavljati se, kupovati i obavljati bankovne transakcije.

Nažalost, napredak tehnologije omogućio je i kriminalcima da zloupotrijebe nove elektroničke usluge na razne načine:

- zaraze vaše računalo *spywareom* i ukradu vaš identitet,
- zatrpaju vam računalo skočnim prozorima i zaraze virusima,
- šalju vam *spam* i lažne e-poruke,
- nagovore vas da otvorite privitak iz lažne e-poruke
- nagovore vas da posjetite lažne stranice i otkrijete im svoje osobne podatke i / ili
- pristupe vašoj bežičnoj mreži.

Uspostava sigurnosnih internetskih protokola zvuči vrlo složeno, no postoji niz jednostavnih tehničkih stvari koje možete i sami napraviti kako biste zaštitili i sebe i svoje podatke na internetu. Ako niste sigurni na koji način to učiniti, obratite se nekome s računalnim iskustvom kome vjerujete ili kontaktirajte pružatelja internetskih usluga.

Što biste uvijek trebali raditi?

Redovito ažurirajte sigurnosna rješenja i preuzimajte potrebne zakrpe

S vremena na vrijeme u programima koje koristite na svom računalu pronalaze se određene slabe točke koje mogu biti meta napada pojedinaca koji razvijaju viruse ili hakera koji žele pristup vašem računalu. Upravo stoga proizvođači softvera povremeno izdaju zakrpe kako bi uklonili slabe točke u softveru.

Sve softverske dopune i zakrpe možete pronaći na stranicama tih proizvođača – uglavnom u rubrici *Download*. Općenito govoreći, najsigurnije su uvijek najnovije verzije operativnih sustava (kao što je, primjerice, *Microsoft Windows*) ili preglednika (primjerice *Internet Explorer* ili *Firefox*).

Instalirajte antivirusne programe

Možda već koristite neki antivirusni program, no da bi bio učinkovit, mora se redovito ažurirati s najnovijim definicijama virusa. Ako niste sigurni na koji način to možete sami napraviti, pogledajte rubriku *Help* programa koji koristite.

Bilo koja datoteka bez nastavka ili s dvostrukim nastavkom – primjerice, wow.jpg.pif – sasvim sigurno je virus i ne bi se uopće trebala otvarati. Osim toga, ne otvarajte privitke koji završavaju s .exe, .pif ili .vbs – to su najčešći nastavci kod virusa.

Veliki je izbor učinkovitih antivirusnih programa koje možete upotrijebiti, a najpopularniji su Kasperski, *McAfee, Trend Micro, Sophos*, *Symantec* i *F-Secure*. Antivirusna zaštita uključena je i u novije verzije Windowsa pod nazivom Windows Defender. No svakako koristite isključivo legitimne stranice jer je na tržištu puno lažnih proizvoda koji će navodno zaštititi vaše računalo, da bi ga na kraju zarazili virusima.

Preglednik mora biti ažuriran

Internetski preglednik možete ažurirati na stranicama njegova proizvođača.

Koristite osobni vatrozid

Osobni vatrozid je još jedno softversko rješenje koje štiti vaše računalo i sadržaje na njemu od zlonamjernih pojedinaca na internetu. Nakon instalacije i konfiguracije, spomenuti vatrozid zaustavlja neovlašteni promet prema računalu i od njega.

Na tržištu postoji cijeli niz učinkovitih programa, a među najpopularnijim osobnim vatrozidima su *Windows Firewall* i *Check Point Zone Alarm* (besplatan) te *McAfee Personal Firewall* i *Norton Personal Firewall*.

Koristite anti-spyware program

Spyware je program koji nadzire i snima način na koji surfate internetom, kao i stranice koje posjećujete. *Spyware* na računalu može završiti bez vašeg znanja ili suglasnosti, a u tom ga se slučaju koristi za otkrivanje vaših osobnih podataka, uključujući lozinke, telefonske brojeve, brojeve kreditnih kartica i broj osobne iskaznice.

Kako bi se *Spyware* onemogućio, potrebno je koristiti *anti-spyware* program. Trenutno dostupni *anti-spyware* programi uključuju *AdAware*, *Microsoft Defender* (besplatan), *Spyware Blaster*, *Spy Sweeper* i *Sunbelt Software Counter Spy*. Svakako ih preuzimajte isključivo s autentičnih internetskih stranica; na tržištu je cijeli niz lažnih proizvoda koji navodno štite vaše računalo, a zapravo ga mogu zaraziti zlonamjernim programima (*spyware*, virus i sl).

Zaustavite neželjenu e-poštu (spam)

Prevaranti ponekad koriste neželjenu e-poštu kako bi pokrenuli prijevaru poznatu kao *phishing*. Naime, njihov je cilj navesti vas da otvorite poveznice (linkove) iz e-poruka kako bi se na vaše računalo instalirao maliciozni program ili vas odvesti na lažnu stranicu. Trebali biste aktivirati filtar koji će svu neželjenu e-poštu automatski preusmjeravati u zasebnu mapu. Nemojte čitati neželjene e-poruke, već ih izbrišite – i to je jedan od načina zaštite od *phishinga*.

Vaša vam banka nikada neće poslati neočekivanu e-poruku s poveznicom (linkom) na jednu od svojih stranica za logiranje (za prijavu u Internet bankarstvo). Ako i dobijete takvu e-poruku, ona sasvim sigurno nije od vaše banke i smjesta je izbrišite.

Budite na oprezu zbog mogućih prijevara

Budite na oprezu jer postoji cijeli niz lažnih internetskih stranica osmišljenih kako bi vas prevarile i prikupile vaše osobne podatke. Ponekad se poveznice (linkovi) na takve stranice nalaze u e-porukama koje navodno dolaze iz financijskih institucija i drugih renomiranih organizacija. Nikada ne otvarajte poveznice u e-porukama – čak i kada se čini da ih je poslala vaša banka.

Čuvajte lozinke na sigurnom

Kada smišljate lozinke, imajte na umu sljedeće:

- držite ih za sebe; **nitko vas u banci neće pitati za vaše sigurnosne podatke za pristup usluzi Internet bankarstva**
- neka ne budu jednostavne i lagane za pogoditi,
- pokušajte osmisliti različite lozinke za različite usluge,
- redovito mijenjajte vaše lozinke i / ili
- nikada ih ne zapisujte.

Budite pažljivi dok surfate

Izbjegavajte korištenje bilo koje internetske usluge koja zahtijeva lozinku u internetskim kafićima i knjižnicama te na drugim javnim mjestima, kako netko ne bi kasnije kopirao vaše podatke i iskoristio ih u nezakonite svrhe.

Odjavite se

Obavezno se odjavite nakon što završite s korištenjem Internet bankarstva te zatvorite preglednik.

Zaštitite računalo lozinkom

Na taj način ćete spriječiti druge da koriste vaše računalo ako ga ostavite bez nadzora ili ako vam ga ukradu.

Ne koristite opciju AutoComplete u pregledniku

Opcija automatskog dopunjavanja (*AutoComplete*) pohranjuje informacije koje ste ranije unosili negdje na internetu, poput vaše adrese ili lozinke. Opcija *Help* na vašem pregledniku pomoći će vam s deaktiviranjem opcije.

Ne pristupajte računalu kao administrator

Nije najpametnije pristupati računalu i koristiti ga kao administrator jer će netko tko dođe u posjed računala na taj način imati gotovo neograničen pristup pohranjenim podacima ili preuzetom softveru i pravima promjene konfiguracije te pokretanja programa uključujući viruse i druge zlonamjerne programe. Puno je bolje napraviti zaseban korisnički račun za redovno korištenje računala, a za potrebe administracije se svaki puta logirati u računalo kao administrator.

Zaštitite bežične mreže

Zahvaljujući bežičnim mrežama računalo možete spojiti na internet bez kabela. Obično vam je za to potreban bežični modem koji koristi radijske signale kako bi podatke prenio do računala u mreži. Bežični modemi dolaze s vrlo niskom razinom zaštite kako bi ih korisnici lakše spojili i aktivirali – no to znači da i druge osobe vrlo jednostavno mogu pristupiti vašem bežičnom modemu pa i računalu koje se spaja na taj modem. Iz tog razloga predlažemo vam sljedeće:

- Pročitajte sigurnosne informacije u priručniku koji dolazi s modemom; brojni modemi dolaze s isključenim sigurnosnim postavkama.
- Koristite vatrozid na svim računalima ili uređajima koji koriste vaš modem.

- Promijenite prvotnu lozinku kako biste pristupili modemu.

Ako niste sigurni kako sve to izvesti, posavjetujte se s nekim kome vjerujete ili kontaktirajte proizvođača bežičnoga modema.

PHISHING („pecanje podataka“ putem e-pošte)

Što je phishing?

Phishing je proces putem kojega prevaranti dobivaju pristup osjetljivim podacima poput korisničkih imena, lozinki ili podataka s kreditnih kartica, slanjem lažnih elektroničkih ili tekstualnih poruka koje izgledaju kao da su ih poslale legitimne organizacije. Poruke najčešće izgledaju kao da dolaze od banaka, popularnih društvenih mreža ili internetskih stranica za prodaju i kupnju.

Phishing se uglavnom izvodi putem e-poruka ili tekstualnih poruka u realnom vremenu (*instant messaging*), u kojima se od korisnika često traži da na lažnim internetskim stranicama (koje su gotovo identične stvarnim stranicama) ostave svoje podatke. Čak i dok koristite legitimne stranice banke, ponekad se na njima mogu pojaviti lažni skočni prozori (*pop-ups*). Čim kliknete na takav prozor ili unesete svoje osobne podatke ili podatke za identifikaciju, vaši podaci odlaze nekom drugom pružatelju usluga ili trećoj strani koja nije vaša banka. To znači da od toga trenutka nadalje netko drugi može pristupiti vašim računima. Postoje e-poruke koje sadrže linkove i žele vas navesti da posjetite web stranice na kojima ćete preuzeti štetne ili maliciozne programe uz čiju pomoć prevaranti mogu doći do vaših podataka i vašeg novca.

Iz privitka se može instalirati i tzv. *ransomware*, a ne samo *malware*.Takvi programi šifriraju vaše datoteke, uključujući glazbu i fotografije, a prevaranti od vas traže „otkupninu“ kako biste ih dobili natrag.

Zaštitite vaša računala i druge uređaje najnovijim sigurnosnim rješenjima i programima najnovijim sigurnosnim rješenjima, te budite na oprezu prilikom otvaranja privitaka ili poveznica (linkova) u neočekivanim e-porukama ili porukama za koje niste sigurni da su vjerodostojne. Svakako napravite sigurnosne kopije svih važnih datoteka u neumreženim mapama te nikada ne plaćajte otkupninu kriminalcima.

E-poruke od vaše banke

Vaša vam banka povremeno može poslati e-poruku s korisnim savjetima ili informacijama o proizvodima ili uslugama, ali vam:

- nikada neće poslati e-poruku koja sadrži poveznicu (link) koja vas izravno vodi na stranicu koja vas izravno vodi na stranicu Internet bankarstva,
- nikada neće poslati e-poruku u kojoj od vas traži da potvrdite podatke o svom bankovnom računu,
- nikada neće poslati e-poruku (ili vas nazvati) kako bi vas pitala za podatke o kreditnim karticama, PIN-ove, kôdove za prijavu (*one time passworde* - OTPove) i kôdove za autorizaciju transakcija (MACove) koje generira token, kao i lozinke,

- nikada neće poslati e-poruku u kojoj od vas traži da potvrdite nedavno obavljenu transakciju.

Ako ste dobili sumnjivu e-poruku koju je navodno poslala vaša banka, proslijedite je vašoj banci, a zatim čim prije obrišite poruku koju ste dobili.

Kako ga prepoznati?

Nestandardna e-adresa

Krivotvorene e-poruke mogu biti poslane s adresa koje su naizgled slične službenim adresama vaše banke, ali ako ih pažljivije pogledate uočit ćete razliku u odnosu na pravu adresu.

Neformalni pozdravi i osjetljiva pitanja

Lažna e-poruka može ali i ne mora biti naslovljena na vas osobno. Može počinjati vašim osobnim imenom ali i npr. sa „Cijenjeni korisniče“ i slično. Obično prevarant od vas traži osobne informacije poput lozinke, podataka o korištenju Internetskoga bankarstva, kontakata ili brojeva kreditnih kartica.

Neodloživi zahtjevi

U lažnim e-porukama često možete naići i na izraze poput ovoga: „Moramo potvrditi informacije o vašem računu“. Na taj vas način žele natjerati da im odgovorite smjesta i bez razmišljanja.

Loš pravopis i oblikovanje teksta

E-poruka može sadržavati gramatičke i pravopisne greške. Nadalje, lažna internetska stranica može imati nešto drugačiji izgled te sadržavati pogrešno napisane riječi. E-poruka može biti napisana na lošem hrvatskom odnosno zvučati kao loš automatizirani prijevod (npr. s Google prevoditelja).

E-poruka bez teksta

Ako primite e-poruku bez teksta, samo s privitkom u prilogu, svakako postupite oprezno. Banka vam nikada neće poslati e-poruku bez ikakva sadržaja.

Neobične poveznice (linkovi)

Iako se poveznica (link) može činiti ispravnom, prije klika svakako provjerite pravu destinaciju na koju vas šalje. Prije nego kliknete, prijeđite mišem preko poveznice (linka) i provjerite kako glasi adresa stranice na koju vas usmjerava. Budući banka nikad neće slati direktni link na stranicu Internet bankarstva, stranici Internet bankarstva uvijek pristupajte direktno (upisom adrese u internet preglednik), a ne putem linka u e-poruci.

Što poduzeti?

- Ograničite količinu osobnih podataka koji su javno dostupni na internetu, uključujući društvene mreže.
- Oprezno postupajte sa svim e-porukama. Povratne adrese ili adrese pošiljatelja mogu se lažirati. Potpunu e-adresu pošiljatelja možete provjeriti tako što ćete mišem prijeći preko naziva pošiljatelja. Zaglavlje e-poruke i poveznica na internetsku stranicu također se mogu lažirati. Prijeđete li mišem iznad poveznice, možete vidjeti potpuno drugačiju stranicu.

- Ne otvarajte poveznice iz neočekivanih ili sumnjivih e-poruka. Upišite adresu u internetski preglednik. Banka vam nikada u e-poruci neće poslati poveznicu na stranicu na kojoj se logirate u svoj bankovni račun ili na stranicu koja od vas traži sigurnosne ili osobne podatke. Budući banka nikad neće slati direktni link na stranicu Internet bankarstva, stranici Internet bankarstva uvijek pristupajte direktno (upisom adrese u internet preglednik), a ne putem linka u e-poruci.
- Nikada ne otvarajte privitke iz neočekivanih e-poruka (pogotovo one s nastavcima .exe, .pif ili .vbf)

Prijavi phishing

Dobijete li lažnu e-poruku, ostanite pribrani jer opasnost ne leži u primanju takve poruke. No nemojte otvarati poveznice (linkove) ili privitke iz takve poruke ili otkrivati podatke o internetskom ili mobilnom bankarstvu. Jednostavno ne odgovarajte na nju i izbrišite je. Ako vas neki od skočnih prozora traži vaše sigurnosne podatke, nemojte ih odavati. Prijavite lažnu e-poruku vašoj banci i pomozite u sprječavanju takvih prijevara.

MALWARE

Malware je zajednički naziv za štetne ili maliciozne programe koje prevaranti koriste kako bi pristupili vašim računalima. Takvi su programi obično skriveni u privicima ili besplatnom sadržaju. Koriste se za niz nezakonitih radnji kao što su krađa osobnih podataka, brisanje ili oštećivanje podataka, stvaranje *botnet* mreža (mreža zaraženih računala) i zaobilaženje sigurnosnih programa.

Postoji cijeli niz različitih štetnih programa, uključujući viruse, trojance, špijunske programe (*spyware*)/reklamne programe (*adware*) i programe za zastrašivanje (*scareware*). Više o štetnim programima i zaštiti od istih donosimo u ovoj rubrici.

- Virusi
- Trojanci
- *Spyware/ Adware*
- *Scareware*

Virusi

Virus je program koji se može reproducirati i koji često sa sobom donosi štetne programe koji mogu naštetiti datotekama i programima na vašim računalima. Nadalje, virusi se koriste za praćenje svega što radite na računalima te omogućavaju nedozvoljen i potencijalno štetan pristup vašim osobnim računalima.

Većina korisnika interneta svjesna je opasnosti koju donose virusi, a zaštita je moguća zahvaljujući raznim antivirusnim programima i vatrozidima. Međutim, osobe koje stvaraju viruse neprekidno pronalaze nove načine širenja virusa na vaša računala.

Kako prepoznati virus/trojanca?

Ako je vaše računalo zaraženo virusom, primijetit ćete sljedeće:

- vaše se računalo ponaša neobično ili neuobičajeno,
- glazba se uključuje sama od sebe,
- na zaslonu računala vidite poruke i skočne prozore ,
- datoteke su promijenjene ili izbrisane,
- vaš tvrdi disk je oštećen ili izbrisan i / ili
- vaše računalo je sporo ili ne reagira.

Kako izbjeći viruse/trojance?

- Na računalo instalirajte antivirusni program/program protiv *malwarea*.
- Provjerite jesu li antivirusni program/program protiv *malwarea* ažurirani.
- Svaki tjedan pregledajte cjelokupno računalo.
- S interneta preuzimajte isključivo sadržaj koji dolazi iz vjerodostojnih izvora. Zapitajte se možete li vjerovati izvoru i izgleda li stranica pouzdano.
- Prije nego što kliknete na 'OK' i date svoju suglasnost, provjerite o čemu je riječ.
- Ne preuzimajte piratske sadržaje (uključujući filmove, glazbu i računalne programe). Iako su besplatni, takvi sadržaji mogu sadržavati štetne programe.
- Pazite da su vaše uobičajene aplikacije i programski dodaci (*plug-ins*) kao što su *Microsoft Office*, *Adobe Acrobat* i *Adobe Flash* uvijek ažurirani i imaju sve sigurnosne zakrpe. Brojne aplikacije mogu se automatski ažurirati.
- **Budite oprezni prilikom plaćanja putem interneta; uvijek provjerite je li stranica na kojoj se nalazite zaštićena. Kako biste bili sigurni da idete na vjerodostojnu stranicu, upišite adresu u preglednik umjesto da kliknete na poveznicu (link).**

Trojanci

Na internetu vas često zatrpavaju zahtjevima za preuzimanjem različitih sadržaja, uključujući pozadine za radnu površinu (*wallpapers*), *screensavere* i *widgete*. Odlučite li se na preuzimanje takvih sadržaja, morate znati da u tom slučaju možda preuzimate trojanca.

Kao što mu i sam naziv govori, trojanac je štetni program koji se pretvara da je nešto što nije i koji u sebi sadrži skriveni program čija je svrha činjenje štete. Trojanac na vašem računalu može napraviti raznu štetu:

- izbrisati ili presnimiti podatke na vašem računalu,
- snimiti udarce po tastaturi kako bi pristupili vašim osobnim podacima,

- deaktivirati vatrozid i antivirusni program i / ili
- instalirati druge viruse.

Budući da trojanci dolaze u različitim oblicima, nema sigurnog načina na koji ih se možete riješiti. Osim toga, neke od njih iznimno je teško ukloniti s računala. Najbolja obrana protiv trojanaca je korištenje ažuriranih antivirusnih programa.

Kako prepoznati virus/trojanca?

Ako je vaše računalo zaraženo virusom, primijetit ćete sljedeće:

- vaše se računalo ponaša neobično ili neuobičajeno,
- glazba se uključuje sama od sebe,
- na zaslonu računala vidite poruke i skočne prozore ,
- datoteke su promijenjene ili izbrisane,
- vaš tvrdi disk je oštećen ili izbrisan i / ili
- vaše računalo reagira sporo ili ne reagira.

Kako izbjeći viruse/trojance?

- Na računalo instalirajte antivirusni program/program protiv *malwarea*.
- Provjerite jesu li antivirusni program/program protiv *malwarea* ažurirani.
- Svaki tjedan pregledajte cjelokupno računalo.
- S interneta preuzimajte samo onaj sadržaj koji dolazi iz vjerodostojnih izvora. Zapitajte se možete li vjerovati izvoru i izgleda li stranica pouzdano.
- Prije nego što kliknete na \\\'OK' i date svoju suglasnost, provjerite o čemu je riječ.
- Ne preuzimajte piratske sadržaje (uključujući filmove, glazbu i računalne programe). Iako su besplatni, takvi sadržaji mogu sadržavati štetne programe.
- Pazite da su vaše uobičajene aplikacije i programski dodaci (*plug-ins*) kao što su *Microsoft Office*, *Adobe Acrobat* i *Adobe Flash* uvijek ažurirani i imaju sve sigurnosne zakrpe. Brojne aplikacije mogu se automatski ažurirati.
- Budite oprezni prilikom plaćanja putem interneta: uvijek provjerite je li stranica na kojoj se nalazite zaštićena. Kako biste bili sigurni da idete na vjerodostojnu stranicu, upišite adresu u preglednik umjesto da kliknete na poveznicu (link).

Spyware / Adware

Spyware je program koji „špijunira“ vaše aktivnosti na internetu, dok je *adware* program koji na vaša računala instalira skočne prozore i oglase. Mnogi od ovih virusa rade i jedno i drugo.

Spyware u najboljem slučaju može biti prilično bezopasan – može prikupiti informacije o vašim navikama surfanja i prikazivati oglase koji odgovaraju onome što vas zanima (*adware*). Pa čak i tada je riječ o svojevrsnom napadu na vašu privatnost i može značajno usporiti rad računala.

U najgorem slučaju *spyware* može biti maliciozan i skenirati vaš tvrdi disk u potrazi za osobnim podacima, poput bankovnih podataka i lozinki, te ih otkriti kriminalcima. Osim toga, može pokušati srušiti vaše antivirusne i *anti-spyware* programe.

Kako prepoznati da je računalo zaraženo spywareom/adwareom?

- Na zaslonu računala pojavljuju se skočni prozori s oglasima (*adware*) čak i kada niste spojeni na internet i ne surfate.
- Početna stranica u vašem pregledniku ili postavke pretraživanja mijenjaju se bez prethodnog upozorenja.
- U vašem se pregledniku pojavila nova, neočekivana i neželjena alatna traka.
- Vaše računalo sve je sporije, a sustav se sve češće ruši.

Kako izbjeći spyware/adware?

Budete li se držali sljedećih savjeta, bit ćete sigurni od *spywarea/adwarea,* ali i brojnih drugih sigurnosnih prijetnji na internetu.

- S interneta preuzmite i instalirajte *anti-spyware* program.
  Korisnicima OS-a *Windows* Microsoft nudi besplatni *anti-spyware* program *Windows Security Essentials*. Drugi proizvođači programskih rješenja nude slične proizvode – bilo koji renomirani isporučitelj računalnih programa može vam preporučiti najprikladnije rješenje za vaš sustav.
- Ažurirajte programe.
  Pazite da su programi na vašem računalu, posebice operativni sustav, ažurirani. Koristite li *Windows*, dopune za svoje programe možete preuzeti a istoj toj stranici možete omogućiti svom računalu da se automatski ažurira, zbog čega nećete morati sami brinuti o preuzimanju najnovijih programskih dopuna i verzija.
- Oprezno surfajte internetom i preuzimajte sadržaj.
  Programe preuzimajte samo sa stranica kojima vjerujete. Ako sumnjate u sigurnost pojedinoga programa, možete upisati njegov naziv u preglednik i provjeriti je li netko prijavio da spomenuti program sadrži i *spyware*.
- Čitajte sva sigurnosna upozorenja, ugovore o licenci i izjave o zaštiti privatnosti prije nego preuzmete bilo koji program.

- Nikada nemojte kliknuti na 'OK' ili 'I agree' u skočnom prozoru, osim ako niste sigurni da znate na što pristajete.
- Budite oprezni s programima za razmjenu besplatne glazbe ili filmova i svakako proučite rješenja koja dolaze u paketu s takvim programima.

Scareware

Scareware ili program za zastrašivanje je vrsta malicioznoga programa koji generira skočne prozore slične porukama operativnoga sustava *Windows* i koji se zatim pretvara da je antivirusni ili *anti-spyware* program, vatrozidna aplikacija ili čistač baze podataka.

Cilj takvih poruka je uvjeriti korisnika da se na njegovom računalu nalazi niz zaraženih datoteka. Korisniku se onda savjetuje kupnja određenoga softverskog rješenja koje će riješiti njegov problem. Problem zapravo uopće ne postoji, a preporučeni program je vrlo vjerojatno pravi *malware*. Ako korisnik povjeruje porukama, ne samo da će izgubiti novac potrošen na beskorisni program, već će se njegovi bankovni podaci vrlo vjerojatno naći u rukama pravih prevaranata. Osim toga, gotovo je nemoguće raditi na zaraženom računalu.

Kako izbjeći scareware?

- Pazite da na računalima uvijek imate instalirane valjane i legitimne antivirusne te *anti-malware* programe. Kontaktirajte svoje pružatelje internetskih usluga i provjerite nude li neka besplatna sigurnosna rješenja ili rješenja koja korisnicima daju pod posebnim uvjetima.
- Nikada nemojte kliknuti na skočne prozore koji tvrde da je računalo zaraženo ili nude skeniranje računala u potrazi za greškama. Gotovo je uvijek riječ o prijevarama.

Prijavite maliciozne programe

Ako na zaslonu vašega računala skočni prozor ili nešto nije onako kako bi trebalo biti, snimite zaslon i pošaljite ga vašoj banci. Ta će nam informacija pomoći u prepoznavanju virusa i drugih vrsta malicioznih programa.