# 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 *McAfee, Trend Micro, Sophos, Symantec* i *F-Secure.* Antivirusnu zaštitu moguće je dobiti i od brendova kao što su *Microsoft Security Essentials, Grisoft AVG Anti-Virus, Antivir, ALWIL Avast* i *ClamWin.* 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.