

Savjeti za sigurno surfanje

Kako bi bili sigurni da vaše računalo i podatke koristite samo vi, važno je pobrinuti se o nekoliko sigurnosnih aspekata. Hrvatska akademska i istraživačka mreža – CARNet vam, s ciljem da vas informira i educira o računalnoj sigurnosti, donosi 10 savjeta za sigurno surfanje.

1. Instalirajte vatrozid na osobno računalo i druge uređaje s kojima pristupate Internetu!

Osobni vatrozid (eng. firewall) jedna je od karika za sigurnosnu zaštitu računala na Internetu. Instaliran, ispravno podešen i redovito ažuriran vatrozid će velikom dijelu zlonamjernih programa onemogućiti pristup vašem računalu.

2. Instalirajte antivirusni program na osobno računalo i druge uređaje s kojima pristupate Internetu!

Antivirusni program je, osim vatrozida, još jedna važna karika za sigurnosnu zaštitu računala na Internetu. Stoga, preporučujemo instalirati ga i redovito ažurirati antivirusne definicije.

3. Redovito ažurirajte operativni sustav osobnog računala i drugih uređaja s kojima pristupate Internetu!

Redovitim ažuriranjem operativnog sustava i primjenom svih preporučenih sigurnosnih zakrpi znatno povećavate sigurnost računala i smanjujete mogućnost kompromitiranja osobnog računala napadom s Interneta.

4. Oprezno prilikom online kupovine!

Prilikom online kupovine provjerite protokol i certifikat na stranici koji se koriste – mora se koristiti https protokol, a certifikat za pristup stranici mora pripadati vlasniku web sjedišta. Neke online trgovine izdaju račun koji je, osim kreditnom karticom, moguće platiti i putem online bankarstva ili pošte. Također, razmotrite mogućnost korištenja zasebne kartice s unaprijed određenim limitom potrošnje samo i isključivo za online kupovinu.

5. Ne šaljite mailom podatke o kreditnoj ili debitnoj kartici odnosno PIN-u!

Nikada nemojte slati podatke o karticama putem e-maila. Vaša banka odnosno kartičarska kuća nikada neće tražiti da im e-mailom šaljete podatke o karticama koje su vam izdali.

6. Nikada ne dijelite korisnički račun s drugima!

Ukoliko nekome ne želite dati svoj identitet, nemojte mu dati niti svoj korisnički račun!

Zapamtite, odgovornost za eventualno počinjenu štetu na Internetu uvijek snosi vlasnik korisničkog računa. Podaci za pristup Internetu (korisničko ime i lozinka) su u tom smislu izjednačeni s identitetom osobe.

7. Redovito mijenjajte lozinke - neka budu dužine barem 10 znakova!

Lozinke za pristup mijenjajte barem jednom mjesečno. Vodite računa o tome da:

- imaju minimalnu dužinu 10 znakova,
- budu skup slučajnih znakova,
- sadrže mala i velika slova te posebne znakove poput `.,!{}[]“#\$%&/()=?*'+.

Ukoliko je problem zapamtiti lozinke koje koristite, na raspolaganju vam stoje tzv. password manager programi za upravljanje lozinkama. U njima na siguran način možete pohraniti lozinke koje koristite za pristup.

8. Objava osobnih podataka na Internetu - razmislite dvaput!

Prilikom objave informacija na Internetu važno je imati na umu činjenicu da sve objavljene informacije postaju javnima. Ukoliko niste spremni objaviti određenu informaciju o sebi u dnevnim novinama, nemojte ju stavljati niti na Internet!

9. Zaštitite kućni wireless!

Ukoliko u kućanstvu pristupate Internetu putem bežične mreže (wirelessa), prilagodite sigurnosne postavke uređaja putem kojega ostvarujete pristup Internetu tako da samo ovlaštena računala mogu pristupati Internetu putem vaše bežične mreže.

Članak je izvorno objavljen na CARNetovom portalu <https://sigurnost.carnet.hr>, gdje se može pročitati više toga o računalnoj sigurnosti.