Korištenje računala na javnim mjestima

Korištenje računala, tableta, pametnih telefona i sl. na javnim mjestima, te korištenje javno dostupnih bazičnih pristupa postalo je uobičajena praksa. Preko 90% osoba ne razmišlja o opasnostima koje se kriju iza te prakse, a od 10% onih koji razmišljaju samo 2% poduzima mjere zaštite.

Krađa uređaja

Ostavljanje ili zaboravljanje uređaja (laptopa, tableta, pametnog telefona) na lako dostupnim mjestima čest je uzrok krađe uređaja, a time i podataka koji su spremljeni na njima. Jeste li ste znali da najveći broj ukradenih podataka dolazi upravo iz zaboravljenih prijenosnih uređaja?

Kako se zaštititi?

- Držite svoj uređaj uvijek uz sebe. Kada to niste u mogućnosti, osigurajte da je uređaj zaključan na sigurnom mjestu.
- Ako odlažete uređaj na neko mjesto, pazite na to tko Vas promatra i prati gdje spremate uređaj.
- Ako spremate laptop u automobil preporučljivo je koristiti zaštitnu bravu (tzv. *Kensington Lock*) za zaključavanje i vezivanje računala u automobilu.
- Zapišite podatke vezane uz vaš uređaj, kao što su serijski brojevi, broj modela i svaki drugi koristan podatak. Čuvajte i račune, jer će dobro doći ako prijavljujete krađu.
- Ugravirajte kontaktne informacije na računalo ili ih napišite na naljepnicu.
- Na aerodromima pazite na uređaj cijelo vrijeme, posebno kada prolazi kroz detektor metala, jer lopovi mogu ugrabiti bilo koju priliku da Vam ukradu isti.
- Provjerite da li vaš uređaj ima zaštitu od krađe kao što je *TheftGuard*, osigurajte da je aktivirana.
- Osigurajte da je neželjen pristup vašem uređaju onemogućen kontrolama pristupa poput lozinki, pametnih kartica, otiska prsta i sl.
- Enkriptirajte svoje podatke.
- Backupirajte redovito svoje podatke.

Korištenje javnih bežičnih mreža

Javne bežične mreže su danas dostupne gotovo na svakom uglu, kafiću, trgu. Hackeri iskorištavaju neznanje korisnika, te bez znanja vlasnika pristupaju uređajima koji se spajaju na javne bežične mreže. To im omogućuje uvid u podatke na samom uređaju, ali i mogućnost instalacije malicioznog softvera koji će prikupljati povjerljive podatke.

Kako se zaštititi i smanjiti stres?

- Prije svega isključite opcije dijeljenja (sharing) koje možda pod normalno koristite kod kuće ili u uredu. Ovo smanjuje opasnost upada na vaše računalo.
- Ukoliko se trebate spajati na poslovne sustave, osigurajte da se na iste spajate VPN-om.
- Izbjegavajte automatsko povezivanje na otvorene bežične mreže. Danas postoje softveri koji Vam omogućuju da se Vaš mobitel, laptop i sl. automatski poveže sa bežičnom mrežom ukoliko je u dometu. Ovo Vas izlaže opasnosti od spajanja na maliciozne mreže.
- Kad god možete, koristite HTTPS konekciju za spajanje na stranice koje zahtijevaju upisivanje Vaših osobnih podataka. Postoji jedan koristan dodatak za Internet pretraživače koji se zove ***HTTPS Everywhere***, koji će se pobrinuti za to.
- Koristite *Two-factor* autentikaciju za prijavu na online servise. To je mogućnost da se prijavljujete koristeći više informacija za prijavu, npr. nešto što znate (lozinka, pin), nešto što imate (dongle, mobitel na koji je poslan kod, token, TAN kartica).
- Uvjerite se da je ime mreže autentično. Ako ste u kafiću, pitajte djelatnike pravo ime mreže. Ponekad hakeri podižu lažne mreže kako bi privukli osobe da se spajaju na njih i na taj način pristupaju njihovim računalima.
- Aktivirajte svoj *Firewall*. Softverski *firewall* može zaštiti vaše računalo od neželjenih upada.
- Koristite redovito nadograđivan antivirusni softver, kako bi otkrili neželjeni softver koji je stavljen na vaše računalo.
- Kada ne koristite internet, isključite svoju bežičnu konekciju.

Korištenje javnih računala

Korištenje računala u Internet kafićima, kao i na aerodromima donosi čitav niz rizika, od bilježenja svih vaših aktivnosti (keylogger softver), do krađe identiteta i povjerljivih informacija.

Kako se zaštititi?

- Prije svega izbjegavajte korištenje javnih računala za pristupanje Vašim online servisima. Jednostavno pretraživanje Interneta je u redu.
- Nemojte kliknuti na "Zapamti moju prijavu" koja omogućuje da računalo zapamti podatke

vezane uz vašu prijavu (korisničko ime i lozinku).
- Koristite anonimno pregledavanje Interneta koje ne ostavlja tragove. U Internet pretraživaču (Firefox, Chrome) otvorite tzv. anonimnu karticu (*incognito tab*), a kod Internet Explorera kada otvorite novu karticu kliknite na InPrivate Browsing.
- Nemojte unositi osjetljive informacije na javnim računalima, jer ne znate što je instalirano na istima.
- Pazite na *shoulder surfing*, tj da netko gleda iza vaših leđa što radite. Ovo generalno vrijedi za korištenje svih uređaja u javnosti, javnih ili privatnih.

Ovo su samo neke smjernice, ali uvijek koristite zdrav razum kod korištenja javnih servisa, budite svjesni opasnosti i zaštitite se.

uto, 2013-07-02 12:15 - Darie Marić**Kategorije:** Sigurnost [1]
Vote: 4

Vaša ocjena: Nema Average: 4 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1288

Links
[1] https://sysportal.carnet.hr/taxonomy/term/30