



Spletna varnost je odvisna od vas samih

Spletna varnost

Splet je zelo enostaven, dostopen in zanimiv. Hitro se naučimo komunicirati in vse se nam zdi blizu. Ne zavedamo pa se določenega tveganja.

Že samo s prijavo v internet smo lahko izpostavljeni varnostnim grožnjam, ki lahko poškodujejo naš računalnik, napadalcem omogočijo, da prevzamejo nadzor nad njim, vdrejo v našo zasebnost ali uničijo naše pomembne podatke. Med vsemi grožnjami varnosti na internetu predstavljajo tovrstni napadalci eno največjih. Njihove tarče niso samo vladne ustanove in finančne institucije, temveč tudi podjetja in fizične osebe.

Zaščita računalnikov pred vdori, s pomočjo katerih lahko nepooblaščen osebe nadzirajo naš računalnik je nujna.

Varnost na internetu je proces, za katerega moramo stalno skrbeti in ga ni mogoče kupiti. Potrebno je stalno izobraževanje uporabnika računalnika o varnosti. Največja napaka večine uporabnikov je nezavedanje o računalniški varnosti in nepremišljeno delo z računalnikom.

Katere nevarnosti nam grozijo, kadar je naš računalnik povezan v internet

Vdor v računalnik je najbolj klasična oblika hekerskega napada. Pomeni nepooblaščen dostop do naše računalniške baze in podatkov v njej. Dva najpogostejša načina vdora sta ranljivost programske opreme in odsotnost avtentikacije (slabo geslo).

Spletne prevare pri katerih vas neznanec s čarobno privlačno ponudbo premami, da mu nakažete denar (najbolj znana so nigerijska pisma, kjer nas želijo napadalci prepričati v sodelovanje).

Spam so sporočila, ki vam vsiljujejo vsebino, katere si ne želite.

Phishing je kraja podatkov, ki storilcu omogočajo dostop do spletnih storitev v vašem imenu in v skrajnem primeru tudi do kraje podatkov ali denarja (npr. kraja podatkov s katerimi dostopaš do spletne banke).

Okužbe z računalniškimi virusi, internetnimi črvi in trojanskimi konji so najbolj razširjena spletna tveganja in služijo predvsem za krajo podatkov in identitete.

Kraja identitete je kraja osebnih podatkov (npr. imena, rojstnega datuma, številke

kreditne kartice) in njihova nezakonita uporaba.

Varnostne napake in brezžična omrežja zaradi katerih lahko napadalci vstopijo v vaš računalnik in pri tem izkoristijo različne pomanjkljivosti programske in strojne opreme.

Napadi za zavrnitev storitev pri katerih napadalci s pomočjo posebnih skript pošljejo preko računalnikov, ki jih imajo pod nadzorom, na napadeni strežnik veliko količino podatkov in predstavljajo veliko nevarnost za ponudnike internetnih storitev, saj lahko začasno onesposobijo strežnik ali del omrežja.

Zaščitite svoj računalnik

Zaščitite računalnik. Namestite požarni zid, preprečite dostop do vsebin, ki niso namenjene javni uporabi, in namestite protivirusni program, vse potrebne popravke vašega operacijskega sistema ter najnovjšo verzijo spletnega brskalnika. Ustrezne posodobitve namestite z uradne spletne strani ponudnika in ne preko nepreverjenih povezav.

Poskrbite za kopije pomembnih podatkov. Redno ustvarjajte varnostne kopije in jih hranite na način, ki omogoča enostaven dostop do njih ob vdoru ali tehnični napaki.

Ločujte poslovno in zasebno. Poslovne računalnike uporabljajte samo v poslovne namene ter poskrbite za varnost podatkov, programske opreme in komunikacije na njih.

Preverite ponudnika. Pred namestitvijo katere koli programske opreme preverite njeno poreklo, proizvajalca ali dobavitelja. Spletne storitve naročajte pri kvalificiranih ponudnikih, ki vam lahko zagotovijo zanesljivo podporo v primeru težav.

Varujte informacije. Previdno objavljate poslovno pomembne informacije in ne odgovarjajte na elektronsko pošto, ki zahteva posredovanje osebnih ali bančnih podatkov.

Zavarujte geslo. Ne uporabljajte preprostih gesel in ne uporabljajte samo enega gesla za vse uporabniške račune. Obdržite gesla zase in jih redno spreminjajte. Gesel ne hranite v bližini vašega računalnika.



Kakšna so varna spletna gesla?

- Vaše geslo naj bo dolgo vsaj osem znakov in naj vsebuje male in velike črke, številke in ločilo (ki ga spletno mesto dovoli uporabiti).
- Če geslo po dolžini ni omejeno, si izberite daljšo frazo namesto ene besede. Uporabite lahko tudi daljši stavek, ki si ga boste zlahka zapomnili, in ga nekoliko spremenite oziroma iz njega vzemite dele po nekem ključu.
- Ne uporabljajte zaporednih črk ali števil, prav tako ne sosednjih tipk na tipkovnici (npr. 12345678 ali asdfghj).
- Ob najmanjšem sumu, da je za vaše geslo izvedel nekdo drug ga nemudoma zamenjajte.

Prijava incidenta

Če ste žrtev goljufije in je prišlo do oškodovanja, to prijavite policiji. Najbolj pomembna podatka pri vsakem prijavljanju kakršnekoli omrežne zlorabe ali varnostnega incidenta sta datum in točen čas dogodka in IP številka oziroma naslov izvora.

Koristni viri:

www.varenspletu.si

www.safe.si

www.spletno-oko.si

www.cert.si