# Novičnik, št. 1
# VARNOST LASTNIH NAPRAV: RAČUNALNIK, TABLIČNI RAČUNALNIK IN MOBILNI TELEFON

Tematiko internetne varnosti lahko razdelimo na štiri dele: zaščita naprav in domačega omrežja, gesla, brskalniki, brskanje po brezžičnih omrežjih. Za vsako od teh kategorij bomo pregledali, kaj vse je treba storiti za doseganje minimalne ravni varnosti, dokler sistem in vsi podatki, ki se prenašajo prek spleta in omrežja, niso popolnoma zaščiteni.

**1) <u>Varnost računalnika, tabličnega računalnika ali mobilnega telefona</u>**

***a) Ali je nameščen protivirusni program? Ali se protivirusni program samodejno posodablja vsak dan?***

Če še niste namestili protivirusnega programa ali če imate program, ki mu je potekla veljavnost in se ne posodablja več, morate ukrepati. Odstranite trenutni protivirusni program in prenesite enega od priporočenih brezplačnih protivirusnih programov. Če želimo protivirusni program oceniti na način, ki je razumljiv vsem, moramo pred odločitvijo upoštevati vsaj 6 parametrov. Pravzaprav je dober protivirusni program tak ki:

- ne sme preveč upočasnjevati računalnika in ne sme imeti veliko prostora v pomnilniku RAM.
- viruse mora zaustaviti, še preden lahko začnejo delovati (aktivno pregledovanje).
- ne sme zaznati preveč lažnih pozitivnih rezultatov, saj vidi grožnje tudi tam, kjer jih ni.
- ne ne traja predolgo za pregledovanje na zahtevo ali občasno samodejno pregledovanje: sodoben SSD mora biti v celoti skeniran v manj kot dveh urah.
- se mora samodejno posodabljati, da lahko takoj zaustavi nove okužbe in prepreči dostop do pomembnih delov sistema.
- mora biti sposoben blokirati neodkrito zlonamerno programsko opremo (grožnje 0-day) in zaznati grožnjo le na podlagi sumljivega obnašanja nekaterih komponent.

Poleg teh parametrov, ki so pri protivirusnih programih zelo pomembni, moramo upoštevati tudi enostavnost uporabe, uporabniški vmesnik, morebitne težave z uporabnostjo ter prisotnost hroščev, napak in nezdružljivosti.

***b) Ali je nameščen požarni zid?***

Če uporabljate sistem Windows 7 in doma brskate po internetu z usmerjevalnikom, ne potrebujete požarnega zidu. Če ga potrebujete, lahko prenesete brezplačen požarni zid, ki bo zaščitil vaše omrežje in preprečil vdore.

***c) Ali je operacijski sistem Windows (ali Mac) posodobljen ter ali se posodablja samodejno in redno?***

Veliko ljudi zanemarja ali pozabi posodobiti Windows sistem s popravki, ki jih Microsoft razpošilja vsak teden. Te posodobitve so vedno varnostni popravki, ki pokrivajo najnovejše luknje, zaradi katerih lahko zlonamerni uporabniki od zunaj vdrejo v računalnik in prevzamejo nadzor nad njim. Preverite, ali je storitev Windows Update aktivna v Nadzorni plošči. Varnostnih posodobitev ne smejo podcenjevati niti uporabniki računalnikov Mac.

***d) Ste pripravili načrt varnostnega kopiranja podatkov, dokumentov in fotografij?***

Da ne bi izgubili datotek, ki jih ustvarjate in shranjujete v računalniku, načrtujte samodejno varnostno kopiranje, da boste imeli dvojno varnostno kopijo. Če nimate preveč podatkov, ki jih morate varnostno kopirati, lahko veliko lažje in hitreje ustvarite spletno varnostno kopijo v storitvah shranjevanja v oblaku, kot sta Dropbox in Skydrive.

***e) Ali posodabljate programe, nameščene v računalniku?***

Podobno kot pri sistemu Windows so tudi pri programih pogosto objavljene varnostne posodobitve. Za tiste, ki to želijo, obstajajo načini za samodejno posodabljanje programov in programske opreme, nameščene v računalniku.

***f) Ali pri prenosu programov pazite, da v postopku namestitve ne namestite tudi druge "priporočene" programske opreme?***

Na žalost je veliko brezplačnih programov opremljenih s sponzorji, tako imenovanim "crapware", v obliki nezaželenih programov, ki se samodejno namestijo.

**2) <u>Varnost brskalnika</u>**

Če je vaš računalnik, tablični računalnik ali mobilni telefon zaščiten pred virusi in zunanjimi vdori, to še ne zagotavlja, da je brskanje varno in zasebno. Veliko ljudi morda ne skrbi za zasebnost, vendar je varnost še vedno najpomembnejša. Ne glede na to, kateri brskalnik uporabljate, mora biti posodobljen na najnovejšo različico in imeti omogočene samodejne posodobitve. Brskalniki, ki so posodobljeni in imajo samodejne posodobitve, so zagotovo Chrome, Firefox, Opera in Microsoft Edge.

***a) Ali ob prijavi z geslom na spletno mesto vedno preverite, ali se naslov začne s https?***

HTPPS je protokol šifrirane povezave in se od običajnega protokola *http* razlikuje po tem, da so vsi podatki, preneseni v protokolu *https*, šifrirani. To pomeni, da podatkov, zapisanih v protokolu *https* ne more prebrati nihče, vključno z upravljavci tega spletnega mesta.

Razširitev brskalnika HTTPS Everywhere opozarja na varna spletna mesta in zagotavlja, da vedno ostanete v HTTPS, kjer je na voljo (glejte članek Navigacija v https na bančnih spletnih mestih, v spletnih trgovinah in Facebooku z varno povezavo).

***b) Ali na prvi pogled prepoznate nevarna spletna mesta, pri katerih morate biti previdni, kam kliknete?***

Če še vedno ne morete na pogled ločiti dobrega spletnega mesta od slabega in ste vedno paranoični ali slabe volje glede katerega koli spletnega mesta, razen najbolj priljubljenih, lahko namestite nekaj razširitev, kot je WOT, da se izognete klikanju na nevarne povezave in sumljiva spletna mesta.

***c) Ali se vedno odjavite, ko se povežete s spletnim mestom iz računalnika, ki ga ne uporabljate samo vi?***

Ne pozabite se odjaviti iz vseh računov, ki jih uporabljate na javnem računalniku ali računalniku, ki si ga delite z drugimi osebami, vključno z družinskimi člani.

***d) Ali poznate osnove spletnih prevar in goljufij?***

Če želite preprečiti phishing, zlonamerno programsko opremo in druge nevarnosti na internetu, morate te nevarnosti poznati.

***e) Ali svoj brskalnik zaščitite pred spletnim sledenjem?***

Kot je bilo že pojasnjeno, preprečevanje sledenja na spletu s strani spletnih mest pomeni blokiranje zbiranja podatkov. To je mogoče z nekaterimi razširitvami, ki jih lahko namestite v brskalnik.

Najvišja raven zaščite in zasebnosti na internetu je anonimno brskanje. Popolnoma anonimno brskanje ni uporabno za vsakogar in ga ni mogoče uporabiti v vseh okoliščinah. Uporabno je lahko, kadar počnete nekaj nezakonitega (vendar dobrega, kot je prenašanje torrentov), kadar ne želite deliti svoje geografske lokacije ali kadar želite ponarediti svoj naslov IP za dostop do blokiranih spletnih mest. Čeprav lahko po internetu anonimno brskate na več načinov, je spletna zasebnost zagotovljena le z brskalnikom TOR.

**3) <u>Varnost gesel, ki se uporabljajo na spletu</u>**

***a) Ali uporabljate zapletena gesla?***

Ena najpogostejših napak, ki jih delajo uporabniki interneta, je uporaba preprostih gesel ali gesel, ki se nanašajo na dejstva ali dogodke iz njihovega osebnega življenja. Vedno morate izbrati gesla, ki jih ni mogoče odkriti, predvsem pa za vsa spletna mesta ustvariti močno geslo, ne da bi komu dali možnost, da ga ugiba (nikoli ne uporabljajte datuma rojstva, svoje najljubše ekipe ali imena svoje žene ali psa).

***b) Ali za vsako spletno mesto uporabljate različna gesla?***

Nikoli ne smete ponovno uporabiti iste kombinacije e-poštnega sporočila in gesla v več storitvah, saj bo heker, če mu bo uspelo priti v ta e-poštni račun, lahko brez težav vdrl v vse osebne račune. Uporabite program za ustvarjanje in upravljanje gesel za spletne račune. Če je mogoče (Dropbox, Google, Gmail in Facebook), lahko uporabite dvofaktorsko preverjanje pristnosti. Za dodatno zaščito preverite dovoljenja aplikacij v omrežjih Facebook in Twitter.

**4) <u>Varnost omrežja</u>**

***a) Ali je vaše domače omrežje WiFi zaščiteno s ključem WPA2?***

Če ni ali če ne veste, kaj je WPA2, morate vedeti, da WPA pomeni Wi-Fi Protected Access ter da sta Wi-Fi Protected Access II (WPA2) in Wi-Fi Protected Access III (WPA3) trije varnostni protokoli in certifikacijski programi, ki jih je razvila zveza Wi-Fi Alliance za zaščito brezžičnih računalniških omrežij.

***b) Ali se zavedate, da je ob vzpostavitvi povezave z odprtim omrežjem Wi-Fi vse, kar počnete, vidno tudi zunaj računalnika?***

Edina stvar, ki varuje varnost gesla na internetu v javnem omrežju wi-fi, je protokol HTTPS, omenjen v prvem vprašanju v drugi točki.

***c) Ali ste preverili mape v skupni rabi v računalniku?***

Kot je bilo dokazano, je vdiranje v računalnike in pregledovanje map v skupni rabi drugih računalnikov zelo enostavno. Zelo pogosto je proces uspešen, ker ljudje pozabijo izključiti skupno rabo map ali celotnega trdega diska v računalniku. Če želite računalnik uporabljati popolnoma anonimno in se povezati v omrežje, ne da bi pustili sledi, lahko uporabite anonimni in zasebni sistem Linux, kot je Tails.

Varnost je pomembna za vse, od izkušenega tehnika do računalniškega analfabeta. Od vas je odvisno, kakšne varnostne ukrepe boste sprejeli, vendar ne pozabite, da je spletna varnost danes prav tako pomembna (če ne še bolj) kot varnost vašega doma.

Ta projekt je financirala Evropska komisija. Ta dokument odraža le stališča projektnih partnerjev, Komisija pa ni odgovorna za kakršno koli uporabo informacij, ki jih ta dokument vsebuje.