ZAŠČITITE SVOJ RAČUNALNIK

z uporabo nasvetov o kibernetski varnosti strokovnjakov podjetja Smart Com

Ne glede na to, ali računalnik uporabljate predvsem za delo ali za osebno rabo, ga želite zaščititi, prav tako pa podatke na njemu ohraniti varne.

Sledite spodnjim korakom, da zmanjšate tveganje za ogroženost vašega računalnika pred varnostnimi grožnjami.

1 *Redno posodabljajte programsko opremo*

Številne varnostne težave se pojavijo, ker programska oprema nima nameščenih najnovejših varnostnih popravkov. Večina programske opreme ima možnost samodejnega nameščanja posodobitev. Če delate z računalnikom, ki ima operacijski sistem Windows, se prepričajte, da ste **vklopili samodejne posodobitve** in tako zagotovili sprotno posodabljanje programske opreme Windows, Microsoft Office in drugih Microsoftovih aplikacij.

Samodejne posodobitve vklopite tudi za programe, ki niso del Microsoft produktov, na primer za **Adobe Acrobat Reader** in druge programe, ki jih redno uporabljate.

Za računalnike Apple Mac uporabite mehanizem za posodobitev programske opreme, ki ga najdete pod zavihkom »System Preferences« (nastavitve sistema) v meniju Apple.

Namestite protivirusno programsko opremo 2

Protivirusna programska oprema je obvezna za vse – za uporabnike sistemov Windows in Mac – je pa seveda treba tudi **protivirusne programe redno posodabljati**. Če uporabljate pomnilniški USB ključ ali zunanje trde diske, vedno preverite, ali vsebujejo viruse, še posebej, če niso vaši.

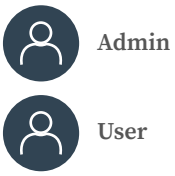
3 *Varno brskajte po spletu*

Izogibajte se obisku spletnih mest s potencialno nedovoljeno vsebino. To še posebej vključuje mesta s pornografsko vsebino ali katero koli drugo sumljivo vsebino! Težava je v tem, da obstajajo **spletna mesta, ki so zasnovana prav z namenom, da vaš računalnik okužijo z virusom**. Številna spletna mesta s pornografsko vsebino si vas vzamejo za tarčo. Uporabljajte sodoben brskalnik, kot je na primer Microsoft Edge, ali najnovejšo različico brskalnika Chrome, ki lahko blokira zlonamerna spletna mesta in prepreči izvajanje zlonamerne kode na vašem računalniku. **Nikoli ne prenašajte, nameščajte ali zaganjajte programske opreme iz nezaupanja vrednih virov**.

4 Previdno pri uporabi e-pošte

Ko pregledujete svojo e-pošto, bodite pozorni na goljufiva sporočila, ki poskušajo ukrasti vaše osebne podatke ali vaš denar. Mnoge od teh prevar so znane kot **prevare z lažnim predstavljanjem ali phishing**. Ne odpirajte sumljivih priponk in ne klikajte na nenavadne povezave v sporočilih. Prevare se lahko pojavijo v e-pošti, tvitih, spletnih objavah, spletnih oglasih, sporočilih ali priponkah in so včasih prikrite ter prikazane kot znani in zaupanja vredni viri.

5 Ustvarite lasten uporabniški račun z omejenimi uporabniškimi pravicami



Tudi če računalnik uporabljate samo vi, si **nastavite uporabniški račun brez skrbniških pravic**. S tem boste omejili škodo, ki jo lahko povzroči zlonamerna programska oprema.

6 Izberite si geslo, ki je varno in ga je težko ugotoviti

Uporabite geslo, ki ima **vsaj osem znakov in vsebuje kombinacijo številk, velikih in malih črk ter posebnih znakov**. Ne uporabljajte prepoznavnih besed ali kombinacij, ki predstavljajo rojstne datume ali druge informacije, ki so povezane z vami. Za vsako spletno mesto, ki ga uporabljate, nastavite drugo geslo.

7 Preverite svoj požarni zid

Požarni zid deluje kot pregrada med računalnikom ali omrežjem in internetom. **Preverjanje požarnega zidu** se morda sliši zapleteno, a v resnici ni. Če imate sistem Windows, pojdite na nadzorno ploščo in v iskalno polje vnesite »požarni zid«. Če je vaš požarni zid »vklopljen« ali »povezan«, potem ste pripravljeni.

Če imate računalnik Apple Mac, kliknite ikono Apple v orodni vrstici, pojdite na »System Preferences« (nastavitve sistema), nato »Security & Privacy« (varnost in zasebnost) in »Firewall« (požarni zid).

8 Izogibajte se tveganim zunanjim napravam

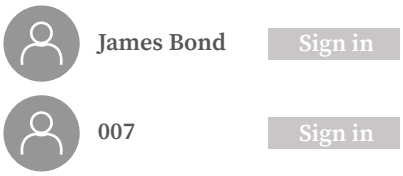
Pomnilniški USB ključi in drugi mediji za shranjevanje so lahko **polni zlonamerne programske opreme**, zato jih ne uporabljajte, če ne pripadajo vam.

Da se izognete okužbi z zlonamerno programsko opremo in virusi, poskrbite, da so vse zunanje naprave vaše ali pa pripadajo zaupanja vrednemu viru.

9 Prekinite povezavo z internetom, kadar računalnik ni v uporabi

Izklopite računalnik čez noč ali v daljših časovnih obdobjih, ko ga ne uporabljate. Če je računalnik vedno vklopljen, je s tem tudi **vidnejša tarča hekerjev**. Izklop računalnika prekine povezavo, ki jo je heker morda vzpostavil z vašim omrežjem in onemogoča morebitna zlonamerna dejanja.

10 Ločite poslovne in zasebne aktivnosti na svojem računalniku



Ko računalnik uporabljate za osebno in ne za profesionalno rabo, se poveča možnost okužb in drugih varnostnih incidentov – filmi, igre, glasba in druge osebne aplikacije so vse povezane s tveganji. Če imate samo en računalnik in želite ločiti službene aktivnosti od zasebnih, si vzemite čas in **ustvarite dva različna uporabniška računa** – enega za delo in drugega za zasebno rabo.

11 Zaščitite svoje domače omrežje

Pomembno je, da zaščitite svoje domače omrežje Wi-Fi. Prepričajte se, da ima vaše domače omrežje Wi-Fi **omogočeno zaščito in da ste spremenili skrbniško geslo usmerjevalnika**. Večina usmerjevalnikov poleg tega omogoča, da »skrijete« svoje omrežje Wi-Fi, kar pomeni, da morajo drugi, ki se želijo povezati z internetom, poznati tako ID vašega omrežja Wi-Fi kot tudi geslo.

Zdaj poznate pomembne korake, ki jih morate upoštevati, da zaščitite svoje osebne podatke in podatke podjetja, ko delate na svojem osebnem računalniku.

Ostanite varni!

30 SMART COM

Že več kot 30 let delujemo na področju IKT in smo eden izmed vodilnih sistemskih integratorjev v Jugovzhodni Evropi.
Z ekipo več kot 70 strokovnjakov in specialistov vzpostavljamo sodobna in zanesljiva komunikacijska omrežja in varnostne rešitve za zaščito pred naprednimi kibernetskimi grožnjami. Z vpeljavo tehnoloških rešitev, ki temeljijo na strojnem učenju in umetni inteligenci ter avtomatizacijo in orkestracijo skrbimo za zaščito IK infrastrukture.

Smart Com d.o.o., Brnčičeva 45, 1231 Črnuče - Ljubljana

www.smart-com.si