
Vaš mese ni bilten za podizanje svesti o bezbednosti informacija

# Da li ste hakovani?

## Uvod

Koliko god da ste zaštićeni, kao i kad upravljate automobilom, pre ili kasnije može vam se dogoditi incident. U tekstu u nastavku saznaćete koji znaci vam mogu pomoći da shvatite da ste hakovani i šta treba da preduzmete u tom slučaju. Što pre postanete svesni da imate problem, veće su šanse da će on biti rešen.

## Znaci koji ukazuju da ste hakovani

- **Antivirusni softver prikazuje upozorenje da je vaš sistem zaražen. Proverite da li je to poruka koju je generisao antivirusni softver koji koristite, a ne iskačući (pop-up) prozor veb sajta koji pokušava da vas prevari da pozovete neki telefonski broj ili instalirate nešto novo. Niste sigurni? Otvorite vaš antivirusni program i proverite šta vam on poručuje.**
- **Pojavio se iskačući prozor koji vas obaveštava da je vaš računar enkriptovan i da morate da platite otkupninu da bi vam fajlovi opet postali dostupni.**
- **Vaš pregledač (eng. browser) samostalno, bez vašeg zahteva, otvara različite veb sajtove.**
- **Vaš računar se često sam isključuje, aplikacije se same zatvaraju, pojavile su se ikonice za aplikacije koje su vam nepoznate ili iskaču nepoznati prozori.**
- **Ne uspevate da se prijavite korišćenjem lozinke za koju ste potpuno sigurni da je ispravna.**
- **Prijatelji vas pitaju zašto im šaljete spam poruke elektronskom poštom, a vi im te poruke nikada niste poslali.**
- **Imate nepoznata zaduženja platne kartice i novac nedostaje sa vašeg bankovnog računa.**

## Šta preduzeti

Ako sumnjate da ste hakovani najbolje je da odmah preduzmete akcije jer će tako eventualna šteta biti manja. Ako je hakovan vaš nalog ili računar na poslu, nemojte pokušavati da sami rešite problem, već ga odmah prijavite nadležnom rukovodiocu i podršci. Ako je hakovan vaš lični računar ili nalog, neki od koraka koje možete preduzeti su sledeći:

- **Promenite vaše lozinke:** Promenite lozinke na vašim računarima i mobilnim uređajima, kao i na vašim nalozima na internetu. Za promenu naloga nemojte koristiti računar koji je hakovan, već neki drugi sistem za koji znate da je bezbedan. U slučaju da imate veliki broj naloga, lozinku prvo promenite za naloge koji su vam najvažniji. Ako vam je teško da pamtite sve te lozinke, koristite menadžer lozinki.

**Finansije:** Ako ste primetili probleme vezano za vašu platnu karticu ili bankovni račun, odmah pozovite vašu banku. Koristite proveren telefonski broj poput onog sa poleđine vaše platne kartice, iz vašeg ugovora sa bankom, ili veb sajta banke koji ćete posetiti sa bezbednog uređaja. U zavisnosti od situacije, razmotrite blokiranje kartice i/ili računa.

**Antivirusni softver:** Ako vas vaš antivirusni softver upozorava na zaražen fajl, postupite po njegovim savetima. Većina antivirusnih rešenja će vam ponuditi i linkove do renomiranih sajtova na kojima možete saznati dodatne informacije o pojedinim vrstama malvera.

**Reinstalacija:** Ako nije moguće ukloniti malver sa računara ili ako želite da budete potpuno sigurni da je vaš računar bezbedan, reinstalirajte operativni sistem. Ne koristite rezervne kopije (bekap) za reinstalaciju, već samo za oporavak vaših fajlova. Ako niste sigurni da reinstalaciju možete da obavite sami, razmotrite da angažujete profesionalnu pomoć. U slučaju da je vaš računar ili mobilni uređaj star, možda će vam se više isplatiti da kupite novi. Kada ste reinstalirali sistem ili kupili novi uređaj, ne zaboravite da ga ažurirate i da kad god je to moguće omogućite automatsko ažuriranje.

**Rezervne kopije.** Za vašu zaštitu je ključno da se na vreme pripremite, što se postiže redovnom izradom rezervnih kopija. Postoje brojna rešenja koja omogućavaju izradu bekapa jednom dnevno ili čak na nekoliko sati. Ma koje rešenje da koristite, ne zaboravite da s vremena na vreme proverite da li se vaši fajlovi zaista mogu povratiti iz rezervnih kopija. Često je oporavak podataka iz bekapa jedini način da vratite vaše podatke nakon hakovanja.

**Zakonska zaštita:** Ako vam neko preti ili sumnjate da ste žrtva krađe identiteta, prijavite to policiji ili Posebnom tužilaštvu za visokotehnološki kriminal.

## Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

## Gost urednik

***Dr Johanes Ulrih*** *(@johullrich na Tviteru) je dekan Odseka za istraživanje SANS instituta, direktor SANS Internet Storm centra i počasni član SANS instituta. Osnivač je DShield kolaborativne mreže senzora i voditelj je podkasta Internet Storm centra na temu IT mrežne bezbednosti koji se svakodnevno emituje.*

## Dodatni materijal

| | |
|---|---|
| Rezervne kopije i oporavak: | https://www.sans.org/u/JGP |
| Pristupne fraze: | https://www.sans.org/u/JGU |
| Menadžeri lozinki: | https://www.sans.org/u/JGZ |
| Šta je malver: | https://www.sans.org/u/JH4 |