

VARNOSTNO OPOZORILO

Spoštovani uporabniki elektronske banke!

Gorenjska Banka v svoje aplikacije vgrajuje najnovejše varnostne standarde, ki veljajo v svetu za poslovanje prek internetnih povezav. Prav s tem namenom je pred časom uvedla tudi elektronski podpis nalogov. Svojim uporabnikom nudi tudi zaščito na pametni kartici, ki trenutno velja kot najvarnejša tehnologija za delo s certifikati.

Kljub temu pa je potrebno opozoriti, da v verigi elektronskega poslovanja nastopate tudi uporabniki s svojimi osebnimi računalniki, ki so izpostavljeni programski opremi, ki se na osebni računalnik namesti prek različnih virusov, t.i. "trojanskih konjev" ali "črvov" in omogoča v določenih primerih prevzem nadzora nad osebnim računalnikom na daljavo ter beleženje in krajo vnesenih podatkov (gesel, imen itd.). Še posebej opozarjamo na nove oblike črva Sober in trojanskega konja Agent.aa, ki je znan tudi pod imeni Trojan-PSW.Win32.Agent.aa in Bancos. Slednji na okuženem osebnem računalniku beleži in pošilja podatke o uporabniških imenih in geslih, vnešenih preko tipkovnice, zajema ekranske slike ipd. Zlikovci lahko ponaredijo tudi spletno stran banke in od uporabnika zahtevajo izvoz digitalnega potrdila in različna gesla. Opozarjamo vas, da tega nikakor ne smete storiti!

Znano je da, proizvajalci operacijskih sistemov za osebne računalnike, od katerih so najpogostejši Microsoftovi Windowsi, izdajajo vedno nove in nove popravke. Prav tako je na trgu na razpolago kopica protivirusnih programov, ki preprečujejo nameščanje zlonamernih kod na računalnike in omogočajo stalno posodabljanje podatkov o novih virusih. Potrebno je, da vsi uporabniki redno posodabljate svoje operacijske sisteme s popravki in uporabljate antivirusne programe.

Predvsem pa je pomembno tudi vaše samozaščitno obnašanje.

Povzetek oziroma priporočila:

- **Redno nameščajte varnostne popravke proizvajalca vašega operacijskega sistema (najbolj uporabljeni so Microsoft Windows);**
- **Če na vašem računalniku še nimate nameščenega antivirusnega programa, svetujemo, da si ga takoj namestite. Skrbite za redno posodabljanje podatkov o novih virusih;**
- **Ne odpirajte elektronske pošte neznanih naslovnikov ali t.i. "spam" elektronske pošte;**
- **Za povečanje stopnje varovanja certifikatov vam priporočamo uporabo pametnih kartic;**
- **Ob nenavadnem obnašanju vašega računalnika, se za pomoč takoj obrnite na strokovnjaka, ki skrbi za vašo strojno in programsko opremo;**
- **V primeru da sumite zlorabo vaših certifikatov, le-to nemudoma prijavite na telefonsko številko 04/2084-312;**
- **Redno kontrolirajte poslovanje na vašem računu;**
- **Najbolj pomembno pa je, da skrbno ravnate s certifikati in pazite na zaupnost gesel.**