# BEZBEDNOSNE PREPORUKE ZA KORISNIKE ELEKTRONSKOG BANKARSTVA

## Generalni saveti i preporuke

### Bezbednost vašeg računara

Bezbedan i ispravan uređaj je jedan od preduslova za sigurno obavljanje transakcija. U nastavku teksta možete pročitati savete za bezbedno konfigurisanje vašeg računara.

- Vaš računar uvek treba da bude ažuriran sa najnovijim ispravkama za operativni sistem i aplikacije koje koristite.
- Instalirajte i konfigurišite antimalver program
- Instalirajte ili uključite zaštitni zid (firewall) kako biste se zaštitili od neautorizovanih pristupa ka vašem računaru
- Za rad na računaru koristite nalog koji nema administratorske privilegije
- Kreirajte snažnu lozinku za vaš nalog (najmanje 8 znakova – mala i velika slova, brojevi i znakovi)
- Redovno pravite bekap svih bitnih podataka u sistemu
- Posebno osetljive podatke možete dodatno osigurati tako što ćete ih enkriptovati na vašem računaru
- Uvek se odlogujte pre nego napustite vaš računar

### Bezbedno korišćenje bežičnih mreža (WiFi)

- Uvek postavite snažne lozinke na vaš bežični uređaj (za pristup uređaju i za povezivanje sa bežičnom mrežom), uređaji koje kupite obično imaju podrazumevane lozinke koje se mogu pogoditi.
- Ukoliko obavljate transakcije preko bežičnih mreža, proverite da li to radite preko bezbednog komunikacijskog kanala (npr. https)
- Budite oprezni kada pristupate nepoznatim bežičnim mrežama, koristite savete iz sekcije Bezbednost vašeg računara.

# Internet Bankarstvo

Prilikom elektronskim pristupa AIK Banci i korišćenja usluga internet bankarstva, potrebno je imati u vidu sledeće savete i uputstva:

- Obavezno se uvek pridržavajte opštih uslova korišćenja koje ste dobili od AIK banke.
- Ne koristite istu lozinku koju koristite za elektronsko bankarstvo na bilo kojim drugim internet stranicama.
- Redovno menjajte svoju lozinku i ne ustupajte je nikad i nikome.
- AIK Banka nikada od vas neće tražiti vaše lozinke (sigurnosne kodove) na bilo koji način (npr. putem telefona ili putem elektronske pošte). Ti podaci su isključivo vaše privatno vlasništvo i ne smete ih otkrivati nikome.
- Čuvajte vaše pristupne podatke na takav način da im je nemoguće pristupiti od strane trećih lica, ili pak ukrasti i/ili javno objaviti.
- Pristupajte svim elektronskim servisima banke isključivo sa zvanične internet prezentacije banke, nikako putem linkova koji se pojavljuju na drugim internet prezentacijama, ili kao rezultati pretrage u pretraživačima interneta.
- Proverite i utvrdite validnost internet stranice elektronskog servisa banke koji koristite, kao i sigurnosne sertifikate klikom na ikonicu u obliku katanca u address bar-u vašeg internet pretraživača.
- Ažurirajte vaš računar najnovijim verzijama i sigurnosnim ispravkama operativnog sistema i internet pretraživača.
- Proveravajte redovno da li je vaš računar zaražen virsuma ili nekim drugim malicioznim aplikacijama koristeći najnovije verzije antivirus i antimalware programskih paketa.
- Ne koristite paralelno internet pretraživač za pristup drugim internet stranicama istovremeno dok ste ulogovani na elektronsko bankarstvo.
- Postoje maliciozne aplikacije koje mogu biti instalirane nenamerno na vaš računar, sa ciljem krađe vaših lozinki. Ukoliko se tokom prijavljivanja na elektronske servise banke sretnete sa bilo kojom neobičnom porukom koja od vas zahteva da ponovo unesete vašu lozinku, prekinite proceduru i izvršite preventivno antimalver skeniranje vašeg računara.
- Nakon završene transakcije obrišite istoriju vašeg internet pretraživača.
- Uvek se odjavite nakon korišćenja računara i obavljanja transakcija.
- Ako elektronsko bankarstvo koristite na kompjuteru koji je dostupan i drugim licima, odjavite se sa aplikacije i obrišite memoriju pretraživača „cache“ ili podesite pretraživač da prilikom zatvaranja automatski briše “cache”. Najbolje bi bilo da koristite opciju pretraživača za rad bez arhiviranja (Internet Explorer – InPrivate Browsing, Chrome – Incognito Window, Firefox – Private Browsing).
- Redovno proveravajte stanje na svom računu i nalog za plaćanje pre same potvrde transakcije.
- Što češće menjajte vaše lozinke a obavezno nakon upotrebe elektronskog bankarstva na javnom kompjuteru, npr. u internet kafiću. Izbegavate logovanje na sistem elektronskog bankarstva na ovim lokacijama.

- Ukoliko je stranica elektronskog bankarstva drugačija od one koju koristite ili ste primetili nešto neobično, prekinite konekciju i odmah obavestite banku.
- Transakcije/plaćanja u elektronskom bankarstvu se autorizuju upotrebom SMS koda koji dobijate putem SMS poruke na Vaš mobilni telefon. Obavezno proverite da li se podaci koji se nalaze u SMS poruci, slažu sa podacima koje vidite u AIK elektronskom bankarstvu. Ova kontrola je neophodna kako biste predupredili eventualnu zloupotrebu ukoliko je Vaš računar zaražen zlonamernim programima.

## Mobilni uređaji

Za bezbedno korišćenje mobilnih uređaja AIK Banka vam preporučuje sledeće:

- Vršite redovan bekap vašeg uređaja i podataka sa njega
- Uključite šifriranje podataka (data encryption) i napravite snažne lozinke za pristup samom telefonu i aplikacijama koje koristite kako bi ste se zaštitili u slučaju gubitka ili krađe vašeg uređaja
- Instalirajte softver za zaštitu od malvera i virusa na vaš uređaj.
- Isključujte bluetooth i wireless konekcije kada ih ne koristite.
- Kada instalirate nove aplikacije na svoj telefon, obratite pažnju na dozvole (permissions) koje tim aplikacijama omogućavaju da pristupe podacima na vašem telefonu. Instalirajte samo aplikacije koje su vam zaista neophodne.
- Redovno brišite cashe memoriju i istoriju veb pregledača (web browser) u vašem mobilnom telefonu
- Aplikacije preuzimajte samo sa zvaničnih veb sajtova određene aplikacije ili sa zvaničnih „prodavnica“ aplikacija (poput Google Play ili App Store).
- Redovno uklanjajte svaku aplikaciju koju ne koristite duži vremenski period.
- Ne uključujte se bez preke potrebe na javne, otvorene i nebezbedne WiFi konekcije.
- Vršite redovno ažuriranje vašeg uređaja kako biste od proizvođača primili najnovije ispravke.
- Preporučujemo da ne vršite prepravke svog mobilnog uređaja („rootovanje“, „jailbreakovanje“, „hakovanje“) jer osim gubitka garancije često te akcije uklanjaju ugrađene sigurnosne mehanizme u operativnom sistemu