SAVETI ZA BEZBEDNO KORIŠĆENJE APLIKACIJE

AIK elektronsko bankarstvo

Ovo uputstvo sadrži osnovna pravila sigurne upotrebe AIK elektronskog bankarstva. Svi korisnici treba da se pridržavaju ovih uputstava kako bi adekvatno zaštitili svoje lične računare i druge uređaje koje koriste za elektronsko bankastvo (na primer mobilne telefone). Posebnu pažnju treba posvetiti zaštiti i pravilnoj upotrebi ličnih podataka i informacija koje su neophodne za korišćenje AIK elektronskog bankarstva, kao što su korisničko ime i lozinka.

Slobodno plaćanje naloga putem AIK elektronskog bankarstva uz upotrebu SMS koda

Transakcije slobodnog plaćanja se verifikuju upotrebom SMS koda koji dobijate putem SMS poruke na Vaš mobilni telefon ili Kodom za plaćanje generisanim u mBanking aplikaciji.

Ukoliko transakcije verifikujete SMS kodom, *obavezno proverite da li se podaci o iznosu i broju računa na koji se sredstva uplaćuju, 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. Za verifikaciju naloga Kodom za plaćanje, preduslov je aktivacija Tokena na mobilnom uređaju. Token je softverski sigurnosni alat koji korisnicima omogućava bezbedne savremene načine autentifikacije i verifikacije naloga za plaćanje. Svako novo plaćanje zahteva generisanje novog Koda za plaćanje.

Mobilni telefon koji koristite za prijem SMS koda ima važnu ulogu u obavljanju plaćanja putem AIK elektronskog bankarstva. Instalirajte samo legalno nabavljene aplikacije na Vaš mobilni telefon. Postoje verzije zlonamernih software-a koji mogu da zaraze praktično bilo koji tip mobilnog telefona.

Ukoliko se nađete u situaciji da Vam stigne poruka u kojoj se od Vas traži da na mobilni telefon, za potrebe AIK elektronskog bankarstva ili drugih servisa Banke, instalirate bilo koju vrstu aplikacija, sistemskih driver-a, sertifikata ili drugog softwarea nemojte to automatski prihvatiti. Obavezno kontaktirtajte kontakt centar Banke na telefon +381 (0)11 785 9999 ili najbližu ekspozituru.

AIK banka trenutno koristi SMS kod samo za potrebe autorizacije transakcija. Nemojte unositi SMS kod za druge namene.

Kako zaštititi lični računar

Antivirusni programi

Neophodno je da na vašem računaru postoji instaliran antivirusni program. Efikasnost u otkrivanju zlonamernih programa (virusa, trojanaca i dr.) direktno zavisi od toga da li se program redovno ažurira antivirusnim definicijama. Taj proces se najčešće obavlja automatski ali je neophodno da proverite da li je ta opcija u programu uključena.

Firewall programi *(*engl. *Personal Firewall)*

To su programi koji sprečavaju neovlašćeni pristup vašem računaru od strane zlonamernih lica. Preporučujemo da na svom računaru imate instaliran i firewall program. Operativni sistemi XP, Vista i Windows 7 ili 8 imaju već ugradjen firewall program. Međutim, i njih je neophodno ručno uključiti.

Redovno instaliranje ispravki i dopuna (engl. *installing of patches and updates*)

Proizvonači kompjuterskih programa vrlo često izdaju ispravke i dopune za njihove operativne sisteme ili druge programe. Ove programske "zakrpe" se izdaju u cilju otklanjanja sigurnosnih ili funkcionalnih mana i neophodno ih je redovno instalirati.

Windows i drugi programi mogu da ovu funkciju obavljaju automatski; proverite da li je ova opcija uključena.

Važno: koristite isključivo dopune i ispravke koje su objavljene na zvaničnim sajtovima proizvonača. Hakeri šalju e-mail poruke ili Vas putem pop-up prozora navode da instalirate lažne dopune i ispravke koje sadrže zlonamerne programe (često se kao razlog navode bezbednosni propusti i hitno reagovanje).

Upotreba legalnih programa

Koristite legalno nabavljene programa i operativne sisteme. Piratske kopije su često zaražene zlonamernim programima (raznim vrstama virusa, trojanaca i dr.).

Obratite pažnju na sledeće!!!

Upotreba elektronskog bankarstva na javnim mestima

Ukoliko koristite e-Banking usluge na javnom mestu uverite se da Vam niko ne "viri preko ramena" dok unosite Vaše korisničko ime i lozinku. Ukoliko ne radite sa svog računara, imajte na umu da računari u Internet kafeima ili kod drugih korisnika mogu biti zaraženi. Preporučujemo da nakon korišćenja AIK elektronsko bankarstvo sa tuđih računara promenite Vašu lozinku kada budete u prilici da to uradite sa „sigurnog" računara. Savetujemo da ne otvarate više paralelnih sesija koristeći istu ili drugu radnu stanicu.

Prevare koje se obavljaju putem telefonskih poziva

Popularan način prevara je pozivanje klijenata putem telefona, pri čemu se kriminalci lažno predstavljaju kao službenici banke i pokušavaju da saznaju Vaše lične podatke (korisničko ime i lozinku, JMBG, broj mobilnog telefona i slično). Često se pri tome pozivaju na bezbednosne razloge ili provere kako bi izgledali manje sumnjivi. Nikada nemojte saopštavati Vaše lične informacije na osnovu ovakvih zahteva. Čak i ako se od Vas traži da „zbog sigurnosnih razloga“ pozovete službenika banke na određeni telefon koji Vam se nudi.

Uvek kontaktirajte kontakt centar Banke putem telefona koji možete naći na zvaničnoj Web prezentaciji.

Izbor lozinki

Uvek upotrebljavajte kompleksne lozinke od najmanje 6 karaktera. Uputstvo za kreiranje lozinke možete videti na strani na kojoj vršite izmenu lozinke u AIK elektronsko bankarstvo. Nemojte upotrebljavati reči koje se mogu naći u rečnicima, kao ni lične podatke koji se mogu pogoditi (npr. imena dece, datum rođenja, naziv firme u kojoj radite i sl.). Redovno menjajte Vaše lozinke, npr. jednom u dva meseca.

Vašu lozinku nikada nemojte saopštavati drugim licima (ni članovima porodice).

Phishing

Ovo je veoma rasprostranjen način prevare. Kradljivci identiteta se predstavljaju, najčešće putem e-mail poruka, kao finansijske ustanove ili kompanije. Šalju spem mejlove ili pop-up poruke da bi vas naveli da otkrijete lične informacije ili lozinke. Nemojte odgovarati na ovakve poruke, pogotovo ne posećujte linkove koji su navedeni u telu takvih e-mail poruka:

- u kojima se zahteva da saopštite Vaše korisničko ime, lozinku ili druge lične informacije. Banka nikada ne koristi e-mail za pribavljanje ličnih ili poverljivih informacija od klijenata.
- koje sadrže linkove ka E-banking aplikaciji
- u kojima od Vas traži da pozovete call centar banke na broj telefona koji se nalazi u poruci i ostavite Vaše lične podatke

Prijava bezbednosnih incidenata

Ukoliko smatrate da ste bili žrtva napada koji su ranije pomenuti ili imate bilo kakve dileme vezano za e-mail ili SMS poruke u kojima se pominje AIK banka obavezno nas kontaktirajte na tel. + 381 (0)11 785 9999.