OPPORTUNITY Banka
Za život prepun mogućnosti!

Bezbedno korišćenje e-banking usluge

Činjenica je da korišćenje e-banking usluge donosi velike prednosti, ali i određene bezbednosne rizike od moguće zloupotrebe ovakvog pristupa bankovnim računima od strane napadača, odnosno hakera.
Kako bi umanjili ove rizike i adekvatno zaštitili svoje računare i ostale uređaje koje koristite za elektronsko bankastvo potrebno je da se pridržavate preporuka i saveta koje Vam u daljem tekstu dostavljamo.

Preporuke i saveti za bezbedno korišćenje e-banking usluge

PIN i kartica sa sertifikatom (Smart kartica)

Da bi bila zagarantovana sigurnost ličnih podataka, svaki korisnik ima jedinstvenu PIN kod koji je samo njemu poznat. Pri svakom korišćenju usluga e-banking aplikacije, neophodno je ulogovati se ponovo.

Medijum za logovanje je **Smart kartica**, na kojoj je snimljen sertifikat neophodan za Vašu zaštitu. On predstavlja autentičnu identifikaciju i njegovim korišćenjem se obezbeđuje mehanizam kojim se sprečava otkrivanje sadržine podataka i njihova promena.

- Posebnu pažnju svakako treba posvetite zaštiti i pravilnoj upotrebi **Smart kartice i PIN**-a;
- Ne dozvolite nikome da vidi Vaš PIN za logovanje, kako bi obazbedili sigurnost poslovanja;
- PIN tretirajte kao lični podatak i nikada ga ne saopštavajte ili pozajmljujete drugim licima. Nikada ga ne zapisujte na ceduljicu, pogotovo ne u blizini mesta gde čuvate karticu sa sertifikatom;
- Broj neuspešnih pokušaja unošenja PIN-a u aplikaciji je tri (3) uzastopna pokušaja, nakon čega će kartica biti automatski trajno blokirana. Za deblokadu se morate obratiti Banci.
- Ako želite da sačuvate Vašu privatnost i novac, **nikada ne ostavljajte Samrt karticu u čitaču kada je ne koristitie za rad. Čuvajte je na sigurnom mestu.**

Prijava bezbednosnih incidenata

- Gubitka kartice odmah prijavite Banci, kako bi Vam se deaktivirao korisnički profil, i time sprečila mogućnost zloupotrebe;
- Takođe, ukoliko primetite nešto neobično u radu Vašeg računara, da je Internet stranica elektronskog bankarstva drugačija od one koju koristite, posumnjate na malicioznost nekog u email-a i SMS poruke u kojima se pominje Opportunity banka, prekinite konekciju i odmah kontaktirajte Banku.

Generalne preporuke i saveti

- Što češće menjajte Vaše lozinke, a posebno nakon upotrebe elektronskog bankarstva na javnom kompjuteru, npr. u Internet kafiću;
- Ne koristite istu lozinku koju koristite za elektronsko bankarstvo na bilo kojim drugim Internet stranicama;
- **Banka nikada od Vas neće tražiti vaše lozinke ili PIN** na bilo koji način (npr. putem telefona ili putem elektronske pošte). Ti podaci su isključivo Vaše privatno vlasništvo i ne smete ih otkrivati nikome;
- Redovno proveravajte stanje na svom računu i nalog za plaćanje pre same potvrde transakcije;
- Pristupajte e-banking servisu isključivo po uputstvu koje ste dobili od Banke, nikako putem linkova koji se pojavljuju na drugim Internet prezentacijama, ili kao rezultati pretrage u pretraživačima interneta;
- Ne koristite paralelno Internet pretraživač za pristup drugim Internet stranicama istovremeno dok ste ulogovani na elektronsko bankarstvo.

OPPORTUNITY Banka
Za život prepun mogućnosti!

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.

- Ažurirajte Vaš računar najnovijim verzijama i sigurnosnim ispravkama operativnog sistema, aplikacija koje koristite i Internet pretraživača *(**važna napomena:** koristite isključivo dopune i ispravke koje su objavljene na zvaničnim sajtovima proizvođača);*
- Koristite najnovije verzije antivirus i antimalware programske alate kako bi redovno proveravali da li je Vaš računar zaražen virsuma ili nekim drugim malicioznim programima;
- Kreirajte snažnu lozinku za Vaš nalog;
- Redovno pravite bekap svih bitnih podataka u sistemu;
- Uvek se odlogujte pre nego napustite Vaš računar;

Bezbedno korišćenje bežičnih mreža (Wi-Fi)

- 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).

Bezbedno korišćenje elektronske pošte

Elektronska pošta je sastavni deo svakog poslovanja, što potencijalnim napadačima predstavlja jednu od osnovnih tačaka za pokušaj vršenja različitih prevara ili kompromitavanja vašeg računara.

Fišing (Phishing)

Fišing ili krađa identiteta predstavlja pokušaj krađe podataka Internet korisnika putem falsifikovane web stranice. Obično se link za takvu stranicu nalazi u e-mail-u ili chat porukama koje se nasumično šalju, u pokušaju da se klijenti prevare i navedu da otkriju informacije na lažnoj web stranici. U tim porukama obično se tvrdi da je neophodno ažurirati ili potvrditi informacije o vašem računu, te se klijenti nagovaraju da kliknu na dati link u elektronskoj poruci/e-mail-u koja ih vodi do lažne web stranice. Sve informacije koje upišete na lažnoj web stranici dospevaju u ruke kriminalaca koje oni zatim koriste u svoje nezakonite svrhe.

Kako izbeći da postanete žrtva fišinga?

Najvažnije je da imate određenu dozu sumnje prema svim neželjenim ili neočekivanim elektronskim porukama koje primite, čak i kada se čini da potiču iz poverljivog izvora. Iako Vam se Banka može obratiti putem elektronske poruke, Banka vam nikad neće poslati poruku kojom od vas zahteva da upišete svoju lozinku ili bilo koje druge poverljive podatke tako što ćete klikom na link posetiti neku web stranicu. Zato nikada nemojte otkrivati svoju punu lozinku ili bilo koje lične podatke.