Bezbednosne preporuke za korisnike digitalnih kanala Banca Intesa

Kako nam je bezbednost podataka naših klijenata prioritet, svakodnevno nastojimo da obezbedimo njihovu sigurnost i poverljivost, primenjujući najsavremenije tehnologije i najviše bezbednosne standarde. S obzirom na to da smo nažalost danas svedoci da se u svetu, a i kod nas, često pronalaze načini za izvršenje određenih prevarnih radnji, u ovom dokumentu Vam dostavljamo preporuke, kako da i Vi zaštitite svoje podatke. Preporuke date u nastavku pomoći će Vam ne samo u obezbeđivanju bezbednog korišćenja elektronskih kanala Banca Intesa, već i u svakodnevnom korišćenju ostalih internet servisa, poput imejla, društvenih mreža i ostalih sadržaja.

Preporuke za kreiranje korisničkog imena i lozinke

- Kreirajte „*jaku*“ lozinku sa što više karaktera, koja obuhvata kombinaciju sa barem jednim velikim slovom, ciframa i specijalnim karakterima.
- Prilikom kreiranja korisničkog imena i lozinke izbegavajte upotrebu reči koje se lako mogu pretpostaviti, poput Vašeg imena i datuma rođenja, odnosno imena i datuma rođenja Vaše dece.
- Nemojte podeliti Vašu lozinku sa trećim licima, pa čak ni sa članovima porodice ili prijateljima.
- Menjajte periodično Vašu lozinku.
- Izbegavajte upotrebu pomagala za automatsko logovanje koja čuvaju korisnička imena i lozinke.

Opšte bezbednosne preporuke

- Ne preporučuje se korišćenje javnih ili neobezbeđenih računara za logovanje u aplikacije elektronskog bankarstva (na primer računare u hotelu ili internet kafeu).
- Svaki put nakon logovanja proverite datum i vreme prethodnog logovanja.
- Proveravajte redovno stanja na računima i detalje transakcija (preporuka je na dnevnom nivou) kako biste potvrdili podatke o plaćanjima kao i ostale podatke o transakcijama, ako primetite bilo koju sumnjivu transakciju, odmah je prijavite banci.
- Ukoliko ne koristite digitalne kanale Banca Intesa za izvršenje transakcija, aktivirajte nalog za uvid u stanja Vaših računa kako biste mogli da pravovremeno identifikujete sumnjive transakcije.

- Registrujte na šalterima Banke Vaš pretplatnički broj mobilnog telefona i aktivirajte SMS usluge za dostavu obaveštenja o promenama stanja po računima i izvršenju transakcija platnim karticama.
- Nemojte koristiti Vaš JMBG, broj računa ili druge lične ili podatke o računu prilikom kreiranja korisničkog imena i lozinke, kao i kod kreiranja kratkih imena Vaših računa u aplikacijama digitalnih kanala.
- Ne ostavljajte računar bez nadzora tokom korišćenja usluga digitalnih kanala Banke.
- Preporučujemo da nikada ne izvršavate bankarske transakcije dok je pokrenuto više različitih internet pretraživača na Vašem računaru.
- Uvek se pravilno izlogujte iz aplikacija digitalnih kanala Banke, i to upotrebom predviđene komande za odjavu. Zatvaranje prozora internet pretraživača ne podrazumeva uvek i odjavu iz sistema (prekid sesije).

Preporuke za izbegavanje Fišinga, Spajvera i Malvera

Sve imejl poruke koje korisniku budu prosleđene od strane Banca Intesa biće upućene sa adrese mail@bancaintesa.rs i zaštićene digitalnim potpisom.

- **Banca Intesa nikada neće putem imejla, SMS-a ili telefona od Vas zahtevati** dostavu, odnosno neće proslediti link za unos **poverljivih podataka** i to: korisničkog imena, lozinke, PIN-a, podataka o platnoj kartici i drugih poverljivih podataka. Ukoliko dobijete takav imejl, SMS ili telefonski poziv, odmah se obratite Banci putem zvaničnog Kontakt Centra (011 310 88 88).
- Ubacite linkove za sajtove Banca Intesa, Banca Intesa Online i Banca Intesa Secure u markere (Bookmarks) Vaših internet pretraživača i pristupajte ovim sajtovima isključivo preko markera, a nikako preko linkova iz sumnjivih imejl poruka.
- Ne otvarajte imejl poruke od nepoznatih pošiljaoca. Uvek budite podozrivi prema imejlovima koji su navodno od finansijske institucije, državne institucije ili neke druge agencije u kojima se zahtevaju podaci o Vašem nalogu, računima ili platnim karticama, odnosno koji zahtevaju verifikaciju naloga ili kredencijale za pristup digitalnim kanalima banke kao što su korisnička imena, lozinke, PIN kodovi i slične informacije. Otvaranje datoteka iz priloga imejla ili kliktanje na linkove iz sumnjivih imejlova može zaraziti Vaš računar malicioznim softverom i omogućiti hakerima potpunu kontrolu nad Vašim računarom, uključujući i pristup svim poverljivim podacima na računaru.
- Nikada ne odgovarajte na sumnjive imejlove, odnosno ne klikćite na linkove sadržane u telu poruke. Kontaktirajte navodnog pošiljaoca ukoliko sumnjate u njegovu legitimnost.
- Instalirajte softvere za anti-virus i firewall, kao i za detekciju Spajvera i Malvera i redovno ažurirajte ove softvere.
- Redovno instalirajte zakrpe za operativni sistem Vašeg računara, ažurirajte operativni sistem i ključne aplikacije.
- Proverite podešavanja Vašeg internet pretraživača i odaberite barem srednji nivo bezbednosti.

Preporuke za izbegavanje „Presretanja imejlova“

Moguće je presretanje poslovne korespodencije između ino-dobavljača i domaćeg kupca (pravno lice), izmena podataka na ino-fakturi i umesto računa ino-dobavljača upis računa trećeg.

- Nemojte koristiti besplatne imejl servise za poslovnu korespodenciju.
- Instalirajte i redovno ažurirajte anti-virusni i firewall softver na Vašem računaru.
- Poverljive i lične informacije kao i poslovnu korespodenciju šaljite isključivo upotrebom zaštićenih imejlova.
- Nemojte koristiti javne računare (internet kafe) za poslovne aktivnosti.
- Pre plaćanja ino-faktura značajnih iznosa, uvek potvrdite i proverite instrukcije za plaćanje sa izdavaocem fakture (ino-dobavljačem).
- Nakon izvršenja plaćanja po osnovu ino-fakture, uvek proverite sa izdavaocem fakture da li je plaćanje uspešno izvršeno.

Preporuke za podešavanje kućne WiFi mreže

Bežična mreža (WiFi) potencijalno može da obezbedi „otvorena vrata“, odnosno neautorizovan pristup Vašoj računarskoj mreži. Ukoliko koristite kućnu WiFi mrežu preporuka je da ista bude obezbeđena na sledeći način:

- Promenite administrativnu lozinku Vašeg WiFi uređaja sa fabrički podrazumevane u jaku lozinku. Sačuvajte novu lozinku u pisanoj formi na bezbednoj lokaciji jer Vam može zatrebati za buduća podešavanja WiFi uređaja.
- Onemogućite udaljenu administraciju vašeg WiFi uređaja.
- Ako vam je prihvatljivo, onemogućite emitovanje SSID-a Vaše bežične mreže.
- Omogućite WPA (ili WPA2) enkripciju i definišite WPA lozinku za pristup Vašoj WiFi mreži.
- Ukoliko će samo poznati računari ili prenosni uređaji pristupati Vašoj WiFi mreži, razmotrite aktiviranje MAC filtera na Vašem uređaju. Svaki računar ili drugi uređaj sa mrežnom karticom ima fabrički dodeljenu jedinstvenu MAC adresu. MAC filter će omogućiti pristup mreži isključivo uređajima sa registrovanom MAC adresom.

Preporuke za mobilno bankarstvo i mToken

- U najkraćem roku Banci prijavite svaki gubitak, krađu, zloupotrebu, neovlašćeno korišćenje, promenu ili gašenje mobilnog pretplatničkog broja i **prenosnog uređaja** (mobilni telefon ili tablet) preko kojeg koristite sredstva za autentifikaciju i usluge mobilnog bankarstva, i to **lično u Banci** ili putem **zvaničnog Kontakt centra Banke**.
- Izbegavajte korišćenje nebezbednih WiFi mreža, kao što su otvorene i javne WiFi mreže, za izvođenje bankarskih transakcija ili uvida u račune. Umesto toga, ukoliko niste u dometu bezbedne WiFi mreže, uvek koristite mobilnu mrežu za prenos podataka u cilju korišćenja usluga mobilnog bankarstva sa Vašeg prenosnog uređaja (mobilni telefon ili tablet).
- Preuzimajte i instalirajte aplikacije isključivo iz legitimnih Apple i Google Play prodavnica.
- Instalirajte i redovno ažurirajte anti-virusni i firewall softver na Vašem prenosnom uređaju.

- Obezbedite Vaš mobilni telefon ili tablet pristupnom šifrom.
- Redovno ažurirajte operativni sistem Vašeg prenosnog uređaja.
- Isključite Bluetooth i NFC kada ih ne koristite. Oni se potencijalno mogu iskoristiti za neautorizovan pristup Vašim poverljivim podacima na prenosnom uređaju.
- Aktivirajte enkripciju na prenosnom uređaju kako biste zaštitili poverljive podatke.