DIGITALNA SIGURNOST KLIJENATA BANKE KOVANICE

Digitalno bankarstvo omogućuje brz i jednostavan pristup financijskim uslugama – bilo kada i bilo gdje. Istovremeno s tim pogodnostima dolaze i brojne prijetnje u digitalnom okruženju.
Sve učestaliji pokušaji internetskih prijevara, krađa identiteta i zloupotrebe osobnih podataka podsjećaju nas koliko je važno odgovorno i pažljivo koristiti online usluge.

U Banci Kovanici, sigurnost naših klijenata ne promatramo samo kao tehnički izazov, već kao zajedničku odgovornost. Aktivno ulažemo u suvremene sigurnosne tehnologije i sustave zaštite, no svjesni smo da je informirani korisnik najsigurniji korisnik. Upravo zato redovito educiramo naše klijente o aktualnim prijetnjama, sigurnosnim savjetima i načinima kako mogu dodatno zaštititi sebe i svoje financije.

Cilj nam je omogućiti ne samo sigurno, već i povjerljivo i pouzdano digitalno iskustvo za svakog korisnika naših usluga.

Najčešće prijetnje na internetu

Na internetu je aktivno mnoštvo različitih prijetnji koje ciljaju korisnike banaka:

- **Phishing napad**i – lažni e-mailovi i poruke koje vas pokušavaju navesti da otkrijete osobne podatke.
- **Vishing napadi** – lažni telefonski pozivi u kojima se prevaranti predstavljaju kao zaposlenici banke.
- **Smishing napadi** – SMS poruke koje sadrže zlonamjerne poveznice.
- **Lažne internetske stranice (spoofing)** – stranice koje oponašaju izgled službenih stranica.
- **Malware** – zlonamjerni softver koji može ukrasti podatke s vašeg računala ili mobitela.
- **Prijevare preko društvenih mreža** – lažni profili koji obećavaju nagrade, kredite ili ulaganja.
- **Quishing (QR phising)** - QR kodovi prevaranata, često postavljeni preko legitimnih QR kodova, s ciljem da korisnika preusmjere na maliciozne stranice

Primjeri pokušaja prijevara

1. Phishing e-mail: "Vaš račun je privremeno blokiran"

Klijent je primio e-mail s naslovom "Sigurnosna provjera Banke Kovanice", s porukom da mora hitno potvrditi svoje podatke zbog sumnjive aktivnosti. Poveznica u poruci vodila je na lažnu stranicu koja imitira bankarsko sučelje.

Pouka: Banka Kovanica nikada ne traži unos osobnih podataka putem e-maila.

2. Lažni poziv službe za korisnike

Prevarant je nazvao klijenta predstavljajući se kao službenik Banke Kovanice i tvrdio da je potrebno odmah potvrditi podatke kartice zbog "hakerskog napada". Tražio je OIB, broj kartice i CVV broj.

Pouka: Pravi zaposlenici Banke Kovanice nikada ne traže ovakve informacije telefonski.

3. Ponuda investicije na društvenim mrežama

Na društvenim mrežama pojavila se lažna "Banka Kovanica Invest" stranica koja je nudila brze povrate ulaganja. Uvjet za sudjelovanje bio je unos osobnih podataka i uplata "startnog iznosa".

Pouka: Banka Kovanica ne nudi investicije putem društvenih mreža i ne traži podatke na takav način.

4. Direktorska prijevara: „Hitna isplata – povjerljivo“

Djelatnik u financijskom odjelu banke primio je e-mail koji je izgledao kao da dolazi od člana Uprave. Poruka je bila kratka i hitna: „Molim te da odmah izvršiš uplatu 9.800 EUR partneru iz ugovora. Trenutno sam na sastanku – ovo je vrlo povjerljivo.“

E-mail je sadržavao stvarno ime i prezime člana Uprave, a čak je imao i gotovo identičnu adresu e-pošte. Isplata je zamalo izvršena, no djelatnik je odlučio dodatno provjeriti telefonski – čime je prevara spriječena.

Pouka:

Napadači se koriste društvenim inženjeringom i pritiskom (hitnost, povjerljivost) kako bi potaknuli djelatnike da djeluju bez razmišljanja. Uvijek provjerite neobične zahtjeve putem drugog kanala komunikacije – telefonski ili uživo.

Primjeri dobre prakse za sigurno digitalno bankarstvo

Da biste dodatno zaštitili sebe i svoje financije, preporučujemo:

- **Uvijek provjerite URL stranice prije unošenja podataka** – adresa mora biti točno https://www.kovanica.hr.
- **Redovito mijenjajte lozinke i koristite snažne kombinacije slova, brojeva i znakova.**
- **Aktivirajte dvofaktorsku autentifikaciju** gdje god je moguće.
- **Nikada ne spremate podatke kartica** na nesigurne aplikacije ili internetske preglednike.
- **Ne otvarajte e-mailove, SMS-ove i poruke nepoznatih pošiljatelja ili sumnjivog sadržaja.**
- **Ažurirajte antivirusne i sigurnosne programe** na svim uređajima koje koristite za internet bankarstvo.
- **Ne koristite javne Wi-Fi mreže** za pristup internet bankarstvu.
- **Zaključajte uređaje PIN-om, otiskom prsta ili drugim sigurnosnim metodama.**

Kako reagirati ako posumnjate na prijevaru?

U slučaju bilo kakve sumnje:

- Ne unosite nikakve podatke i ne otvarajte sumnjive poveznice.
- Ne razgovarajte dalje s osobama koje traže osjetljive podatke.

Odmah kontaktirajte Banku Kovanicu putem službenih kanala ukoliko sumnjate na krađu ili zlouporabu Vaših pristupnih podataka:

Telefonski broj: 060/403-403

E-mail: kovanica@kovanica.hr

Web stranica: https://www.kovanica.hr/

Vaša sigurnost je zajednička odgovornost.

Hvala što s nama gradite sigurno digitalno okruženje!