OSTANITE BEZBEDNI - ZAŠTITITE SE OD PHISHING INTERNET PREVARA

Dragi korisnici,

Znate da uvek brinemo o vama, a posebno o bezbednosti vaših ličnih i finansijskih podataka. Zato vam sada šaljemo preporuke na koji način možete da ostanete sigurni u sajber prostoru i zaštitite se od različitih vrsta onlajn prevara.

Šta sve podrazumeva online prevara (phishing) i kako je prepoznati?

Phishing predstavlja pretnju po onlajn bezbednost i on se najčešće realizuje kroz kanale komunikacije kao što su: lažni sajtovi, imejl, društvene mreže, SMS, Viber ili WhatsApp poruke.

Cilj je da se kroz ove kanale prikupe vaše lične i poverljive informacije, poput korisničkih imena, lozinki, brojeva kreditnih ili debitnih kartica i drugih osetljivih podataka. Ističemo da je izuzetno važno da izbegavate da čuvate korisničko ime i lozinku u pretraživačima, kao i da ih delite sa drugima.

U nastavku su praktični saveti za prevenciju od internet prevara:

1. Pažljivo proverite imejl adrese:

Pre nego što otvorite bilo koji link ili prilog u imejlu, pažljivo proverite imejl adresu pošiljaoca. U onlajn prevarama često se koriste adrese slične adresama banke i drugih institucija, kako bi se došlo do podataka korisnika. Ako vam imejl deluje sumnjivo ili je adresa nepoznata, budite oprezni.

2. Obratite pažnju na nepotpune ili loše napisane imejlove.

Phishing imejlovi često sadrže gramatičke greške, nepravilno formatiran tekst ili nepotpune informacije. Ozbiljne organizacije ne šalju takve imejlove.

3. Ne delite poverljive informacije putem imejla.

Privatne ili državne institucije ili organizacije, a posebno banke, nikada neće tražiti da im putem imejla dostavite osetljive podatke, kao što su lozinke ili brojevi (računa, platnih kartica, JMBG i drugih poverljivih informacija), datumi isteka ili sigurnosni kodovi debitnih/kreditnih kartica. Nikada ne odgovarajte na takve zahteve.

4. Budite oprezni sa linkovima.

Postavite kursor miša preko linka kako biste videli ispis adrese na koju vodi taj link. Ukoliko nije ista adresa kao ona navedena u tekstu ili ne počinje sa https, onda je potrebna opreznost.

5. Proverite SSL Sertifikate (https:// i ikonica katanca).

Kada posetite veb stranicu na kojoj unosite poverljive podatke, uverite se da je stranica sigurna tako što ćete proveriti da li ima SSL sertifikat. Ako ima, takva stranica sadrži "https://" pre URL adrese i ikonicu katanca u pregledaču. Ukoliko ih nema, ne preporučujemo vam da poverljive podatke ostavljate na takvim veb stranicama.

6. Koristite dvofaktorsku autentifikaciju.

Veliki broj sajtova i aplikacija nudi logovanje korišćenjem dvofaktorske autentifikacije, što podrazumeva da se nakon unosa korisničkog imena i lozinke, šalje i dodatni kod kroz SMS ili imejl. Kod se može generisati i kroz neku od aplikacija za dvofaktorsku autentifikaciju. Aktivirajte dvofaktorsku autentifikaciju (2FA) za svoje onlajn naloge gde god je to moguće, jer to dodatno otežava da se desi internet prevara, čak i ako preuzmu vaše korisničko ime i lozinku.

7. Izbegavajte čuvanje lozinki u pretraživačima i deljenje sa drugima.

Ne čuvajte korisnička imena i lozinke u pretraživačima, jer to može omogućiti pristup vašim podacima onima koji koriste isti uređaj ili u slučaju spoljnog napada (hakovanja). Takođe, nikada ne delite svoje lozinke sa bilo kim, čak ni sa prijateljima ili kolegama.

8. Edukujte se.

Redovno pratite savete i informacije o trenutnim phishing taktikama. Što bolje razumete kako napadi funkcionišu, to ćete lakše prepoznati potencijalne pretnje.

Važno je da budete pažljivi i informisani kako biste zaštitili svoje poverljive podatke od internet prevara. Zapamtite, prevencija je ključna.
Za Mobi Banku, bezbednost ličnih i finansijskih podataka svih naših korisnika, saradnika, partnera i zaposlenih predstavljaju najveći prioritet u poslovanju.

Uvek tu uz vas,

Mobi Banka