# Informacije o internet sigurnosti

## Bezbednosne preporuke

### Zaštitite svoje podatke i novac

IT bezbednost postaje sve važnija. Imajući u vidu brzinu i lakoću kojom ostvarujemo internet konekciju, putem bežičnih ili mobilnih mreža, posebnu pažnju moramo usmeriti na siguran pristup mejlu, elektronskom bankarstvu i društvenim mrežama i na taj način sprečiti krađe informacija i novca.

Osim toga što se sa izuzetnom pažnjom odnosimo prema podacima naših klijenata i primenjujemo najviše bezbednosne standarde u poslovanju, pozivamo vas da i vi **upoznate moguće načine zloupotrebe i uz naše savete i preporuke sprečite da do njih dođe**.

Ne smemo se opuštati, a posebno tokom trenutne situacije usled pojave virusa Covid-19, koja je veoma pogodna za pokušaje prevara i phishinga.

Pročitajte preporuke za sigurno korišćenje platnih kartica prilikom plaćanja na prodajnim mestima i internetu, kao i opšte preporuke za zaštitu vaših podataka.

**SAVETI**

- Instalirajte na svoj računar adekvatne bezbednosne programe, antivirus i firewall softver i redovno ih ažurirajte.
- Kada vam stigne email koju niste očekivali, a u poruci se nalazi link ili prilog, kontaktirajte pošiljaoca preko drugog komunikacionog kanala ukoliko sumnjate u njegovu legitimnost.
- Preporučujemo vam da budete obazrivi prilikom preuzimanja besplatnih programa, kao i da proverite preko interneta njihovu legitimnost i iskustva drugih korisnika.
- Ukoliko primetite da je prilikom posete nekom internet sajtu inicirano preuzimanje nepoznatog fajla, prekinite proces preuzimanja i napustite taj sajt.
- Redovno kreirajte rezervne kopije (back-up) podataka sa vašeg računara i čuvajte ih na lokaciji koja nije dostupna napadaču (npr. eksterni hard disk).
- Da li je lozinka sigurna? Bolje da imate više od jedne koju koristite. Nikada ne koristite istu lozinku za različite naloge. Uvek zaštitite svoju elektronsku poštu, profile društvenih mreža, korisničke profile povezane sa uslugama elektronskog bankarstva, kreditnim karticama, finansijskim proizvodima različitim lozinkama. Zaista, ako bi haker napao jedan od vaših naloga, mogao bi pristupiti i drugim vašim korisničkim profilima odnosno nalozima koristeći istu lozinku.
- Ako je protokol HTTPS, na sigurnom ste. Kada veb lokacija zatraži da preuzmete podatke ili se prijavite sa korisničkim nalogom i lozinkom, proverite da li se na levoj strani adrese nalazi zelena ikona katanca, a zatim HTTPS protokol, koji možete videti u samom nazivu veb adrese kojoj pristupate (npr. https://www.google.rs)
- Dokument koji niste tražili? Rešite ga se! Ako primite mejl sa neobičnim linkom ili prilogom (na primer dokumente overene kod notara ili druge vrste koje ne koristite u okviru svog posla), budite oprezni i nemojte im pristupati ili preuzimati.

- Reči su važne i treba da budu tačne. Obratite pažnju na naslov i telo mejla: ako sadrži gramatičke greške ili nije u skladu sa vašim maternjim jezikom, obrišite ga bez otvaranja. Mnogi hakeri pokušavaju da uđu u profile korisnika u raznim delovima sveta sa tekstovima prevedenim preko onlajn servisa koji tek treba da se usavrše i zato je sasvim lako videti da su ih kreirali sumnjivi izvori.
- U slučaju datoteka sa sumnjivim ekstenzijama, pravilo je: obrišite ih! Kada primite prilog, uvek proverite nastavak imena datoteke pre nego što ga otvorite. Pored datoteka sa ekstenzijom .exe, virusi su sakriveni u lažnim fakturama, kaznama, obaveštenjima o isporuci itd. Takođe se brzo šire i obično se šalju kao .doc, .xls i .pdf datoteke. Budite veoma oprezni prema datotekama koje nemaju jedno od uobičajeno korišćenih ekstenzija: ako ih dobijete, ne pokušavajte da shvatite o čemu se radi, već ih odmah obrišite.
- Nikada se ne opuštajte: čak i najbezazleniji mejl može da bude opasan. Jedna od strategija koju hakeri koriste je strategija širenja virusa putem mejlova sa sumnjivim prilozima, na primer, lančana pisma. Kroz priloge koji se preuzimaju i instaliraju, to su upravo vrste poruka koje omogućavaju hakerima da uđu u vaše korisničke profile. U tom slučaju nikada ne odgovarajte ili ne prosleđujte ove mejlove: obrišite ih i ispraznite kantu.
- Odlazak na odmor je u redu, ali obaveštavanje svakoga može da vam kreira probleme. Ako nećete biti u kancelariji, podesite Outluk servis za automatsko odgovaranje samo za primaoce u okviru vaše kompanije, ali ne i za spoljne primaoce. Tako ćete izbeći da potencijalnim hakerima date do znanja da vas neko vreme neće biti, odnosno da vaš nalog neće biti pod vašom kontrolom u periodu odsustva.
- Pazite na svoj račun: u slučaju sumnjivih transakcija obratite se svojoj banci. Barem jednom nedeljno proverite transakcije na svom bankovnom računu i, ako je moguće, aktivirajte SMS obaveštenja koja vas odmah obaveštavaju o bilo kojoj transakciji koja uključuje odliv sredstava sa računa. Ako primetite bilo kakve transakcije ili troškove koji nisu uključeni, odmah se obratite banci i zatražite pojašnjenje, a u slučaju operacija koje nisu tražene, odmah prijavite slučaj, pružajući bilo kakve informacije koje bi mogle pomoći da se utvrdi izvor kršenja.
- Linkove za sajt OTP banka i link za pristup OTP elektronskom bankarstvu unesite u markere (Bookmarks) vaših internet pretraživača i pristupajte ovim sajtovima preko markera, a nikako preko linkova iz sumnjivih imejl poruka.
- Višing i Smišing su najnoviji oblici sajber prevara: budite na oprezu kada su u pitanju SMS, WhatsApp poruke ili lažni kontakt centri.

## Komunikacija sa bankom

Zaštitite se od onih koji se predstavljaju kao zaposleni OTP banka (na internetu ili preko telefona) i od vas zahtevaju podatke koje nakon toga mogu upotrebiti na neovlašćen način.

**PAŽNJA:**

Treće lice vas može kontaktirati telefonom i od vas zahtevati podatke kao što su npr. korisničko ime, lozinka, PIN, podatke s platne kartice (broj u kombinaciji s datumom važenja) koje nakon toga može upotrebiti na neovlašćen način.

Takođe, može vas kontaktirati i preko emaila ili SMS-a i tražiti vam poverljive podatke. Ove poruke su, grafički i sadržajno, vrlo slične onima koje koristite u komunikaciji s bankom ili drugim institucijama, i

za cilj imaju da od vas ukradu poverljive i osetljive podatke i izvrše lažne finansijske transakcije i prevaru.

**NAPOMENA:**

Predstavnici Banke, nikada neće zahtevati od vas preko SMS-a, imejla, društvenih mreža ili drugih vidova komunikacije, da unesete ili saopštite sigurnosne kredencijale (lozinke i PIN-ove za internet/mobilno bankarstvo ili platne kartice).

Takođe, vrlo je važno da:

- Obezbedite svoj mobilni telefon ili tablet s pristupnom šifrom i aktivirate opciju šifrovanja / enkripcije podataka na uređaju.
- Instalirate antimalware softver na vaš mobilni uređaj.
- Isključite Bluetooth i NFC kada ih ne koristite.
- Neovlašćenim pristupom vašem telefonu nepoznato lice može zloupotrebiti podatke s uređaja.

Molimo vas da u najkraćem roku Banci prijavite svaki gubitak, krađu, zloupotrebu, promenu ili gašenje mobilnog pretplatničkog broja ili tableta preko kog koristite sredstva za identifikaciju (autentifikaciju) i OTP uslugu mobilnog bankarstva.

Bežična mreža (WiFi) potencijalno može da obezbedi „otvorena vrata" vašem računaru i omogući zloupotrebu podataka. Iz tog razloga vas molimo da se pridržavate sledećih saveta:

- Izbegavajte upotrebu vašeg imena i datuma rođenja, kao i vaše dece ili supružnika, prilikom kreiranja korisničkog imena i lozinke.
- Izbegavajte upotrebu pomagala za automatsko logovanje, koja čuvaju korisničko ime i lozinku.

## Bezbedno korišćenje kartica na internetu

Kada se odlučite da neku kupovinu obavite preko interneta, najpre se raspitajte o reputaciji trgovca/sajta na kojem kupujete.

Istražite naziv sajta i ako je bilo nekih problema sa kupovinom preko tog sajta, velike su šanse da je neko već na internetu pisao o tome. Ako je u pitanju sajt sa komisionom prodajom, u nekom delu svakog sajta obično stoji informacija o reputaciji svakog prodavca. Kada god je moguće, plaćajte karticama radije nego doznakom, zato što imate dodatne mogućnosti za reklamacije u kojima može da vam pomogne banka. Uvek pročitajte uslove za vraćanje robe i uslove garancije.

Ako na sajtu postoji broj telefona, pozovite taj broj kako biste se uverili da broj, odnosno kompanija, postoji. Pošaljite email prodavcu kako biste se uverili da je adresa postojeća. Sajt koji nema ni svoj domen, već koristi javne besplatne email servise poput gmail, yahoo i sl, je sumnjiv i treba da ga izbegavate. Izbegavajte internet prodavnice koje ne sadrže podatke o adresi sedišta kompanije. Nemojte da vrednujete prodavca prema atraktivnosti sajta – kvalitetan sajt se danas pravi veoma lako.

Pre nego što unesete broj kartice, uverite se da ste na tzv.sigurnom sajtu, čija adresa počinje sa https: (kod takvih sajtova često ćete uočiti sliku katanca u desnom donjem uglu browser-a). Ako je ponuđeno, odaberite korišćenje escrow servisa. Nemojte da verujete u sigurnost sajta samo na osnovu takve izjave ispisane na sajtu. Ako nakon plaćanja posumnjate u legitimnost i reputaciju sajta čak i nakon plaćanja, odnosno ako sumnjate da je broj vaše platne kartice kompromitovan, odmah obavestite banku da blokira i zameni karticu.

Pažljivo čuvajte podatke o svojim karticama i računima.

Ukoliko sumnjate da ste bili meta napada na bilo koji od gore navedenih nacina, molimo vas da kontaktirate našu korisničku podršku.

**OSNOVNI POJMOVI VEZANI ZA SIGURNOST PODATAKA**

Digitalni sertifikat To je vrsta "elektronske" lične karte koju dodeljuje nezavisno sertifikaciono telo kojim se potvrđuje identitet korisnika smart kartice, sa ciljem da se licu koje prima poruku omogući da dešifruje sadržaj poruke. Svrha korišćenja digitalnog sertifikata jeste obezbeđivanje sigurnosti kod plaćanja.

Digitalni potpis Digitalni potpis predstavlja elektronski potpis koji se koristi za autentikaciju identiteta pošiljaoca poruke, ili potpisnika dokumenta. Takođe se koristi kao dokaz da originalni sadržaj poruke ili dokumenta nije izmenjen od trenutka kada je dokument potpisan. Njime se obezbeđuje autentičnost poruke, njena neporecivost i integritet podataka.

Mere predostrožnosti: Ukoliko se posumnja da je sertifikat vlasnika kartice na bilo koji način kompromitovan, to moze da znači da postoji realna opasnost od falsifikovanja potpisa na dokumentima (nalog za plaćanja itd).