

BEZPEČNÉ POUŽÍVÁNIE PLATOBNEJ KARTY

I. Chráňte si kartu

- ❖ Kartu po prevzatí z nepoškodenej obálky podpíšte.
- ❖ Nastavte si limity na karte také ako skutočne využijete.
- ❖ Kartu nikdy nedávajte z ruky, ak nemáte dôveru v obchodníka alebo sa vám zdá podozrivé zariadenie, radšej zvolte inú formu platenie.
- ❖ Pravidelne si kontrolujte stav a obraty na účte cez internetové, mobilné bankovníctvo alebo si aktivujte službu zasielania informačných SMS správ.
- ❖ Zapište si telefónne číslo na blokovanie karty v prípade straty, krádeže alebo zneužitia karty **ihneď ju bezplatne zablokujte** na telefónnom čísle: **+421 2 5966 8230**.

II. Strážte si PIN

- ❖ PIN si nikdy nezapisujte a v žiadnom prípade ho nenoste napísaný spolu s kartou.
- ❖ Nikomu ho neprezrádzajte a neposielajte e-mailom alebo nezašlávajte na internetové stránky.
- ❖ Chráňte si PIN pred odpozorovaním prekrytím ruky pri jeho zadávaní.

III. Platby

- ❖ Pro platbách v reštauráciách, hoteloch nespúšťajte kartu z očí.
- ❖ Nedovoľte, aby si obchodník zapísal údaje o karte, hlavne CVV/CVC kód vytlačený na karte.
- ❖ Po skončení platby skontrolujte si správnosť zaplatenej sumy.
- ❖ Odporúčame platiť len u dôveryhodných obchodníkov označených VISA Secure alebo Mastercard ID Check so 3D Secure bezpečnostným štandardom.
- ❖ V každom okamihu platby musí byť na platobnej bráne v adresátovom riadku ikona zámku a po kliknutí naň sa zobrazí platný certifikát overujúci identitu stránky.
- ❖ Nikdy nereagujte na e-mailové alebo telefonické naliehania na prezradenie identifikačných údajov či overovacích kódov, ktoré Vám prišli do SMS správy ani ak adresátom sú zaručené adresy a vaši známi, nikdy neviete, či ich účty nie sú napadnuté hackermi.
- ❖ SMS kód s nikým nezdieľajte, ak ste dostali SMS kód a neviete dôvod kontaktujte nás **na čísle: +421 2 5966 8230**.
- ❖ Vyvarujte sa zadávaniu údajov karty na verejných WiFi sieťach, nedôveryhodných počítačoch.

IV. Peňaženky Apple Pay, Google Pay, FitBit Pay a Garmin Pay

- ❖ Zariadenie (telefón, hodinky, tablet) zabezpečte PIN, biometriou alebo TouchID, FaceID alebo iným spôsobom, podľa zariadenia (napr. nastavením vzoru na odomykanie zariadenia).
- ❖ Nezdieľajte s nikým číslo platobnej karty, CVV/CVC, verifikačný kód, ktorý Vám banka zasiela formou SMS správy.
- ❖ Pokiaľ Vám príde SMS správa s potvrdením, že Vaša platobná karta bola digitalizovaná a nie ste si vedomí, že by ste svoju platobnú kartu digitalizovali, túto skutočnosť ihneď nahláste na telefónnom **číisle +421 259 668 230**.
- ❖ Dbajte, aby bolo vaše mobilné zariadenie zabezpečené antivírusovým programom a aktualizovaným operačným systémom výhradne od výrobcu mobilného zariadenia.
- ❖ Využívajte len dôveryhodné dátové pripojenie – mobilný operátor alebo zabezpečená WiFi sieť. V prípade straty mobilného zariadenia s aktívnou aplikáciou s uloženou platobnou kartou ihneď bezplatne zablokujte na telefónnom **číisle: +421 2 5966 8230**.
Banka zablokuje vašu fyzickú platobnú kartu a súčasne aj virtuálnu platobnú kartu vo vašom zariadení.

Buďte o krok vpred a poznajte dôležité informácie!

Phishing: podvodné e-mailové útoky, ich cieľom je vylákať údaje ku karte a účtu (napr. PayPal, eBay, Skype, Google)

Pharming: zadanie citlivých údajov na presmerovanú falošnú stránku

Smishing: podvodné SMS odkazujúce na falošnú stránku, kde je požadovaný od klienta potvrdzujúci overovací kód z SMS správy na vykonanie platby alebo registrácie v mene klienta napr registrácia do ApplePay

Skimming: neoprávnené získanie kartových údajov a PIN prostredníctvom skimmovacieho zariadenia na bankomate alebo POS termináli, následne dochádza k výrobe duplikátu karty, s ktorým sa realizujú výbery hotovosti z bankomatov v zahraničí.

E-commerce odcudzenie údajov karty z dátových sietí (transakcie cez internet)

Family fraud: zneužitie údajov karty blízkym okolím klienta ako sú rodinní príslušníci, kolegovia, priatelia, napr. na Internetových hrách

MO/TO a Key Entry: únik údajov karty z e-mailových, faxových a telefonických objednávok, prípadne z manuálneho zadania transakcie cez POS terminál (napr. rezervačné systémy – hotely, letenky, reštaurácie)