BEZPEČNÉ POUŽÍVANIE PLATOBNEJ KARTY

Držiteľ platobnej karty je od momentu jej získanie alebo prevzatia povinný vykonať všetky primerané úkony na zabezpečenie ochrany personalizovaných bezpečnostných prvkov vrátane citlivých platobných údajov (PIN, číslo karty, platnosť karty, CVV/CVC kód).

I. Chráňte si kartu

1. Karta je viac ako hotovosť. Správajte sa k nej ako k peniazom.
2. Kartu si strážte a noste ju oddelene od svojich dokladov.
3. Kartu si ihneď po prevzatí podpíšte na podpisový prúžok.
4. Karta je vydaná iba pre vás a je neprenosná.
5. Kartu nikomu nepožičiavajte (ani rodinným príslušníkom).
6. Číslo karty nikdy a nikde bezdôvodne nezverejňujte.
7. Kartu chráňte pre mechanickým poškodením alebo pôsobením magnetického poľa.
8. Po skončení platnosti karty sa riaďte pokynmi banky. Ak ju neodovzdáte banke, zničte ju.
9. V prípade straty, krádeže alebo zneužitia karty, **ihneď ju zablokujte** na telefónnom čísle **+421 2 5966 8230, ktoré je vám k dispozícii nepretržite 24/7**.
10. Aktivujte si **Zabezpečenú internetovú platbu** (3D Secure) ako ochranu pred zneužitím alebo neautorizovaným použitím vašej karty v prostredí internetu.

II. Strážte si PIN

1. PIN je osobné identifikačné číslo slúžiace na identifikáciu platobnej karty pri jej použití v bankomate alebo POS termináli.
2. PIN sa naučte naspamäť.
3. **PIN si nikdy nezapisujte a v žiadnom prípade ho nenoste napísaný spolu s kartou**.
4. PIN nikomu neprezrádzajte – príbuzným, polícii, iným orgánom alebo dôveryhodne pôsobiacim subjektom.
5. **PIN je diskrétny údaj** – banka si ho nikdy nepýta. Nedajte sa oklamať vylákaním PIN cez podozrivé e-maily alebo stránky. Podozrivú aktivitu čo najskôr nahláste svojej banke.
6. Chráňte si PIN pred odpozorovaním – pri platbách v obchodoch alebo pri výberoch z bankomatov. Pri jeho zadávaní zabráňte priamemu výhľadu na klávesnicu.
7. Buďte obozretní pred odpozorovaním PIN pri jeho zobrazovaní cez služby Internet/Business bankingu.
8. Zmena PIN je možná kedykoľvek pomocou bankomatu ktorejkoľvek banky.
9. Nevhodný PIN je typu 1234 (za sebou idúce čísla) alebo 6666 (rovnaké čísla), **nepoužívajte ich**. Dbajte, aby bol 4 miestny PIN náhodný.
10. Pri opakovanom nesprávnom zadaní PIN (3 krát) sa karte z bezpečnostných dôvodov obmedzí jej ďalšie používanie. Karta je znovu použiteľná nasledujúci deň od jej obmedzenia.

III. Platby cez internet

1. Platťte len u dôveryhodných obchodníkov označených **Verified by Visa** alebo **Mastercard SecureCode**.
2. Platťte **Zabezpečenou internetovou platbou** formou zaslaného bezpečnostného SMS kódu (3D Secure) na váš mobilný telefón. SMS kód s nikým nezdieľajte. V prípade, že vám je doručený SMS kód, ale žiadnu transakciu ste nevykonávali, **KARTU OKAMŽITE BLOKUJTE** na telefónnom čísle **+421 259 668 230, ktoré je Vám k dispozícii nepretržite 24/7**.
3. Nastavte si primeraný limit pre internetové platby. Limit pre internetové platby si môžete kedykoľvek bezplatne meniť cez služby Internet/Smart bankingu.
4. Ak nevykonávate platby cez internet, môžete ich deaktivovať cez služby Internet bankingu.
5. Vyvarujte sa zadávaniu údajov karty na verejných WiFi sieťach, nedôveryhodných počítačoch.
6. Chráňte citlivé kartové údaje – číslo karty, platnosť karty, CVV/CVC kód (bezpečnostný kód na zadnej strane karty). Buďte obozretní komu ich poskytujete.
7. Skontrolujte si svoju registráciu alebo uloženie čísla karty v systémoch obchodníka, čím udeľujete súhlas obchodníkovi iniciovať opakované kartové transakcie (recurring).

IV. Bezkontaktné transakcie

1. Jednotlivá bezkontaktná transakcia bez zadania PIN je možná do max. výšky 20 EUR, bezkontaktná transakcia nad 20 EUR sa autorizuje zadaním PIN.
2. Z bezpečnostných dôvodov banka nastavila maximálny limit pre bezkontaktné transakcie do výšky 60 EUR za sebou opakovaných jednotlivých transakcií. Limit je možné obnoviť vykonaním kontaktnej transakcie a zadaním PIN.

V. Výber hotovosti z bankomatu

1. Všímajte si ako vyzerá bankomat.
2. Sústreďte pozornosť na podozrivé úpravy, poškodenie alebo netradičnú zmenu vzhľadu bankomatu.
3. Podozrivý bankomat bezodkladne / ihneď nahláste banke na telefónnom čísle **+421 259 668 230, ktoré je Vám k dispozícii nepretržite 24/7**.
4. Overte, či sa na bankomate nenachádza kamera na zosnímanie vášho PIN.

VI. Podozrivý obchodník

1. Pri platbách u obchodníka kartu nespúšťajte z očí.
2. Buďte prítomní pri každej platbe.
3. Nedovoľte, aby karta bola mimo váš dosah na čo i len krátky čas.
4. Akékoľvek **podozrivé správanie** obchodníka **nahláste banke** na telefónnom čísle **+421 259 668 230, ktoré je Vám k dispozícii nepretržite 24/7**.

VII. Majte prehľad o svojich platbách

1. Kontrolujte odchádzajúce transakcie – na predajnom doklade skontrolujte sumu a uchovajte si doklad o transakcii.
2. Autorizačné SMS – majte prehľad o všetkých svojich transakciách. Aktivujte si ich cez **Internet Banking**.
3. Pravidelne si kontrolujte pohyby na účte cez služby Internet/Smart bankingu a porovnajte si ich so zrealizovanými transakciami.
4. Podozrenie na neobvyklú transakciu **ihneď nahláste** na telefónnom čísle **+421 259 668 230, ktoré je Vám k dispozícii nepretržite 24/7**.
5. Pri podozrení na zneužitie si zablokujte svoju cez služby Internet/Smart bankingu.

VIII. Reklamácia

1. Reklamácia je písomná žiadosť na prešetrenie spornej transakcie.
2. Reklamáciu môžete podať v lehote najneskôr do 13 mesiacov od dátumu uskutočnenia spornej transakcie.
3. **Bezodkladne** podajte reklamáciu v prípade podozrenia na zneužitie, straty/krádeže. V prípade zneužitia karty je **nevyhnutná je trvalá blokácia**.
4. Pri podaní reklamácie je potrebné presne špecifikovať spornú transakciu, zdokladovať ju a prípadne dodať iné vyžiadané doklady od banky.

IX. Dôležité informácie

1. Phishing – podvodné e-mailové útoky, ich cieľom je vylákať údaje ku karte a účtu (napr. PayPal, eBay, Skype, Google).
2. Skimming – neoprávnené získanie kartových údajov a PIN prostredníctvom skimmovacieho zariadenia na bankomate alebo POS termináli, výroba duplikátu karty, s ktorým sa následne uskutočňujú výbery z bankomatov v zahraničí.
3. E – commerce – odcudzenie údajov karty z dátových sietí (transakcie cez internet).
4. Family fraud – zneužitie údajov karty blízkym okolím klienta ako sú rodinní príslušníci, kolegovia, priatelia a podobne (najčastejšie u obchodníkov s internetovými hrami).
5. 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).