

Zneužitie karty pri výbere peňazí: Situácia zlepšila, klienti by mali byť stále obozretní (+kroky bánk)

20.3.2025 - Filip Maxa | Ringier Slovakia Media

Skimming, podvodná technika získavania údajov z platobných kariet, bol v minulosti jedným z najrozšírenejších druhov podvodov pri používaní bankomatov, s ktorými sa mohli stretnúť klienti. Obzvlášť rozšírený bol v najmä v zahraničí. Záškodníci využívali sofistikované zariadenia na kopírovanie údajov z platobných kariet. Následne vyrábali zväčša duplikáty kariet, ktoré zneužívali na výbery hotovosti alebo nákupy.

V posledných rokoch však vďaka technologickému pokroku a prísnejším bezpečnostným opatreniam skimming postupne ustupuje. Banky na Slovensku uviedli, že implementovali ochranné mechanizmy. Hrozba skimmingu však úplne nezmizla, a preto je dôležité, aby boli klienti pri používaní platobných kariet stále opatrní.

Čo je skimming

Skimming je technika, pri ktorej podvodníci umiestnia na bankomat alebo platobný terminál špeciálne zariadenie schopné skopírovať údaje z platobnej karty. Často sa používa aj skrytá kamera alebo falošná klávesnica na zaznamenanie PIN kódu. Takto získané údaje môžu byť následne použité na výrobu duplikátu karty a jej zneužitie.

Ako sa chrániť pred skimmingom:

Slovenská sporiteľňa: Vieme vypnúť bankomat

Najväčšia slovenská banka zaznamenala pokles prípadov skimmingu. Hovorí, že to je aj kvôli antiskimovacím zariadeniam na bankomatoch. V prípade podozrivých transakcií dokáže systém okamžite zareagovať a vypnúť bankomat.

Banka tiež podporuje využívanie mobilných zariadení na výbery z bankomatu ako bezpečnejšiu alternatívu.

„V prípade pokusu o skimming dostávame okamžite hlásenie z bankomatu a následne vypíname daný stroj a posielame servis. Odporúčame klientom používať výber mobilom, ktorý funguje už niekoľko rokov a zároveň **v priebehu marca spúšťame bezkontaktné výbery** pomocou karty alebo mobilu, či iného zariadenia, ktoré zníži pomer skimmingu,“ spresnila Slovenská sporiteľňa.

365.bank: Treba byť obozretný

Banka tvrdí, že vďaka zavedeným opatreniam zaznamenáva menej prípadov skimmingu. Spolieha sa na kombináciu čipových kariet, bezkontaktných čítačiek a ďalších technologických riešení na zvýšenie bezpečnosti. V prípade podozrenia banka odporúča klientom okamžite kontaktovať políciu aj samotnú banku.

„Na našich zariadeniach využívame kombináciu konštrukčných a technologických opatrení na

identifikáciu a aktívne minimalizovanie rizika skimmingu. Podozrivé zariadenia môžu mať rôzny vzhľad, často sú dokonca nerozpoznatelné," popisuje 365.bank.

Pokus o skimming dokáže inštitúcia odhaliť pri fyzickej návšteve bankomatu v rámci dopĺňania hotovosti a servisu. Tiež má nastavené opatrenia na monitorovanie a elimináciu určitých typov podozrivých transakcií.

Fio banka: Pokusy sme nezaznamenali

Fio banka má na Slovensku najmladšiu vlastnú sieť bankomatov. Uvádza, že na jej zariadeniach zatiaľ neboli zaznamenané žiadne pokusy o skimming. Banka zabezpečuje bankomaty antiskimmingovou ochranou a kamerovými systémami so záznamom.

„Podozrivé zariadenia by si mohol všimnúť len veľmi pozorný a technologicky zdatný

klient, pretože útočníci zariadenia umiestňujú priamo do kontaktnej čítačky kariet. Ak má klient podozrenie, že na bankomate je podozrivé zariadenie, mal by kontaktovať prevádzkovateľa bankomatu," informovala banka.

Klientom odporúča nastavovať geografické obmedzenia pre platby kartou a radšej vyberať hotovosť bezkontaktné. Prevádzkovateľ bankomatov však samozrejme dopredu nevie, akú techniku útočník použije a ako efektívne ju ovláda. Pravidelne však pracovníci banky bankomaty kontrolujú.

„Všetky naše bankomaty sú vybavené najmodernejšou technológiou na detekciu pokusov o neoprávnené zásahy," informuje banka.

Tatra banka: Minimálny výskyt skimmingu

Tatra banka v stanovisku uviedla, že eviduje minimálny výskyt skimmingu a spolieha sa na pokročilé bezpečnostné riešenia. Monitoruje podozrivé transakcie a v prípade potreby zablokuje kartu skôr, než dôjde k zneužitiu. Klientom odporúča používanie manažovateľných limitov na kartách.

„Na celej sieti bankomatov máme nainštalované antiskimmingové bezpečnostné riešenie, ktorého úlohou je zamedziť alebo významne sťažiť páchatelom zaznamenať údaje z platobnej karty. Súčasne naše servisné spoločnosti pravidelne kontrolujú integritu bankomatov," vysvetľuje banka.

Okrem toho doplnila, že vzhľadom na vývoj nie je možné jednoznačne popísať, ako presne tieto zariadenia vyzerajú. Terajšie skimmingové zariadenia môžu byť podľa banky pre klienta prakticky neviditeľné. Napriek tomu vraj problémy v jej sieti neeviduje.

„Dlhodobu neevidujeme žiadny alebo len minimálny počet pokusov o transakcie pravdepodobne zoskimovanými platobnými kartami," dodala.

Kolko kyberútokov denne zachytáva popredný slovenský operátor? Prečo DDoS útoky namiesto ústupu dramaticky narastajú a ako mení AI taktiku kybernetických útočníkov? Aké služby ponúkajú telekomunikační operátori v oblasti bezpečnosti? Na tieto a ďalšie otázky odpovedáme v našom podcaste.

UniCredit Bank: Neevidujeme takéto prípady

Inštitúcia podľa svojich slov využíva integrované zariadenia, ktoré znemožňujú získanie údajov z platobných kariet klientov. Skimming na svojich bankomatoch neeviduje, no varuje klientov, aby si

vždy všímali, ako a kde svoju kartu používajú.

Podozrivé zariadenie pritom zvyčajne podľa banky vzhľadom kopíruje dizajn bankomatu v oblasti čítačky kariet.

„Spôsob použitia platobnej karty je vždy na rozhodnutí klienta, alebo na prostredí, kde klient svoju kartu chce použiť a aké možnosti mu prostredie ponúka. Bezkontaktné výbery sú tie najbezpečnejšie,“ odkázala UniCredit Bank.

VÚB banka: Desať prípadov ročne

VÚB eviduje veľmi nízky počet prípadov skimmingu – asi desať prípadov za celý rok. Banka sa spolieha na pravidelné kontroly bankomatov a neustále monitorovanie transakcií. V prípade podozrivých aktivít dochádza k okamžitému blokovaniu kariet a informovaniu klientov.

„Ak si klient všimne niečo neštandardné alebo podozrivé na bankomate, mal by telefonicky kontaktovať banku, ktorej bankomat patrí, a zotrvať pri danom bankomate do príchodu pracovníka banky alebo servisnej spoločnosti na bankomaty,“ uviedla VÚB.

Posledné verzie podvodných zariadení boli podľa banky pre bežného klienta ťažko rozoznatelné.

ČSOB: Neeviduje ich vôbec

ČSOB uvádza, že v posledných rokoch neevidovala žiadne prípady skimmingu cez svoje bankomaty alebo pri kartách svojich klientov.

Spolieha sa na pokročilé bezpečnostné softvérové a hardvérové riešenia. Klientom odporúča pri používaní bankomatov chrániť zadávanie PIN kódu a v prípade podozrenia okamžite kontaktovať banku alebo políciu.

„ČSOB disponuje viacerými preventívno – bezpečnostnými nástrojmi na monitoring a ochranu klienta pred takýmito typmi podvodu,“ doplnila.

Tento článok publikujeme v rámci aktivity Global Money Week.

<https://zive.aktuality.sk/clanok/YsRwkN5/zneuzitie-karty-pri-vybere-penazi-situacia-zlepsila-klienti-by-mali-byt-stale-obozretni-kroky-bank>