Čo je to skimming?
Skimming je metóda, ktorá spadá medzi podvody s platobnými kartami. Nie je tak rozšírená, ako napríklad odcudzenie platobnej karty cez internet, ale patrí medzi najrozšírenejšie metódy podvodu.

Páchatelia sú považovaní za špičku v organizovanom zločine, ich techniky sú dokonale prepracované, pričom dodnes sa podarilo zadržať len do desať páchateľov, ktorí úspešne okrádali ľudí práve cez klonovanie platobných kariet. Medzi ich arzenál patria priam dokonalé náhrady skutočných zariadení, často sú schopní prekryť aj veľkú časť bankomatu, aby obeť nepostrehla, že sa ju niekto snaží okradnúť. Obete sú (práve kvôli veľmi nízkej informovanosti o jednoduchosti celého postupu) prekvapené, ako prišli o veľkú časť svojich peňazí napriek tomu, že platobnú kartu nikdy nespustili z rúk...

Ako to funguje?
Páchateľ potrebuje v zásade dve veci: vašu platobnú kartu alebo údaje z jej magnetického prúžku a váš PIN kód.

- Údaje z magnetického prúžku karty ľahko skopíruje zariadením (tzv. ***skimmer***), ktoré nalepí na otvor pre vkladanie karty, umiestnený na bankomate. Alebo do otvoru vloží niečo, čo platobnú kartu zablokuje a bankomat ju klientovi po použití nevydá. Keď klient odíde, páchateľ si ju z bankomatu jednoducho vyberie...
- PIN kód môže páchateľ nasnímať skrytou kamerou, ktorú umiestni na bankomat, prípadne do falošnej krabičky s letákmi, či do akéhokoľvek objektu, ktorý je v blízkosti bankomatu. Zložitejšie a aj ťažšie odhaliteľné je, keď páchateľ na klávesnicu bankomatu umiestni jej kópiu (tzv. ***pin pad***), ktorá PIN odchytí pri zadávaní. Používateľ nič netušiac zadá svoj PIN, mysliac si, že ho zadáva na klávesnicu bankomatu...

Ako skimming vyzerá v praxi - všimli by ste si podozrivý bankomat?

Vybrali by ste si peniaze z tohto bankomatu?

Objavené nahrávacie a komunikačné zariadenie.

otvor pre kartu s **falošnou** krytkou (skimmerom)

pôvodný **bezpečný** otvor pre kartu

odstránená falošná krytka

Je vám tento bankomat podozrivý?

Bolo na ňom objavené falošné čítacie zariadenie.

Zdá sa vám to tu bezpečné?

Správna odpoveď je - **nie**

A tu je **kamera** odhalená

Detailný pohľad na kameru odzadu.

Zariadenie je malé

Kopírovacie zariadenie zvonku často vyzerá ako súčasť bankomatu. Niektoré sú dokonca dosť tenké na to, aby sa zmestili do otvoru pre platobnú kartu. Stačí, aby boli trošku väčšie, ako je platobná karta a trošku menšie ako otvor...

Pri veľmi pozornom pohľade by však malo byť viditeľné, že bankomat vyzerá inak ako bežne. Umelohmotný kryt, do ktorého sa zasúva karta, je napríklad o niečo väčší ako bežný.

Takýto neprofesionálny pokus by ste mali byť schopní odhaliť.

Naopak tento skimmer už menej nápadný ani nemohol byť.

Falošné krytky mávajú podobný dizajn ako bankomaty, na ktorý sú použité, takže je ťažké odhaliť zmenu.

Pôvodná bezpečná klávesnica bankomatu.

Všimli by ste si túto **falošnú** klávesnicu umiestnenú nad ňou?

Niekedy útočníci namiesto falošnej klávesnice na bankomat namontujú **celú novú spodnú časť** (na obrázku vpravo), ktorá zachytáva PIN kódy ľudí používajúcich bankomat. Je to ťažko odhaliteľné. Riešením je bankomat prezrieť, či na ňom nenájdete uvoľnené spoje, alebo hýbajúce sa časti. Buďte veľmi obozretní a pri najmenšom podozrení použite iný bankomat.

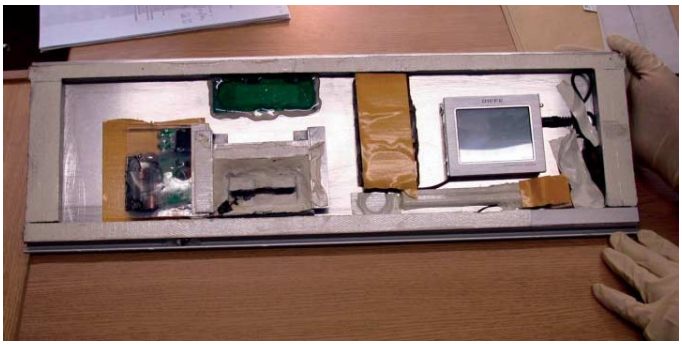
Miniatúrna kamera (na obrázku vpravo) nahrávajúca klávesnicu je umiestnená do medzery medzi nálepkami zobrazujúcimi prijímané platobné karty.

Je tak malá, že na fotografii ju vôbec nie je vidieť.

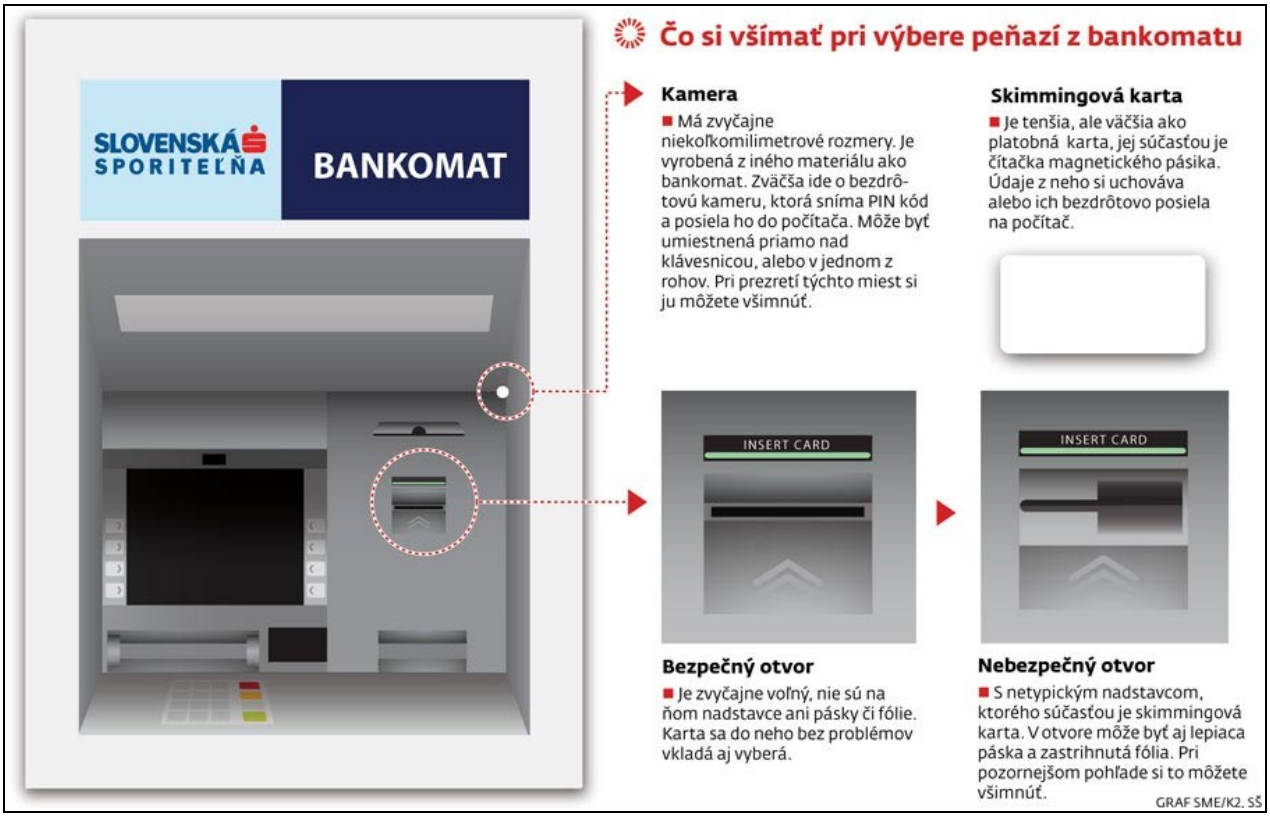
Originálny bankomat.

Bankomat **s falošným celým predným panelom.** Všimli by ste si rozdiel?

Pohľad na odmontovaný falošný panel.



Vnútri sa nachádzala kompletná elektronika vrátane batérií.



Ani podávač bankoviek nie je dobré brať na ľahkú váhu

1. Ani bližší pohľad na bankomat nám nepovie, že bol upravený.

2. Jemné odreniny po krajoch podávača bankoviek môžu niečo naznačiť, no bežný klient si ich nevšimne.

3. Ide o falošný kryt podávača bankoviek a na týchto obrázkoch vidíte jeho odstraňovanie.

4. Ešte jeden obrázok falošného krytu, ktorý slúži k zadržaniu bankoviek. Bankomat čiastku vydá, ale vy sa k nej nedostanete.

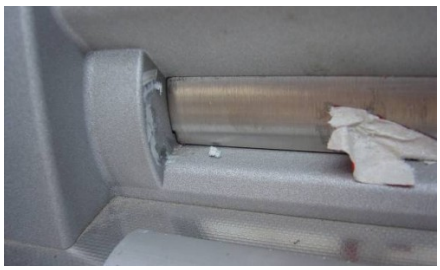
5. Odstránený falošný kryt - na vnútornej strane je obojstranná lepiaca páska slúžiaca ku prilepeniu bankoviek.

6. Profil falošného krytu presne kopíruje originál. A tvári sa veľmi nenápadne.

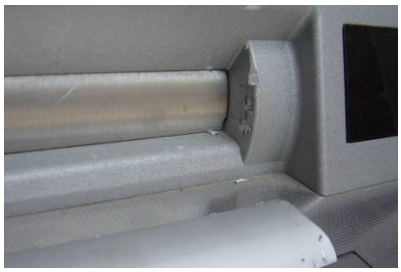
7. Pohľad na samotný falošný kryt.

8. Keď teraz porovnáme kryty podávača, už vidieť že sú tam rozdiely. No na začiatku to tak jasné nebolo...

9. Jemné odery po stranách podávača bankoviek, nás môžu varovať pred možným neoprávneným zásahom do bankomatu.



10. Takéto neobvyklé úkazy nás môžu varovať, že sa s bankomatom deje niečo nekalé.



Ďalší spôsob útoku na bankomaty – technika zastrihnutej fólie

Páchateľ zasunie špeciálne zastrihnutú fóliu do priestoru snímacieho zariadenia bankomatu. Po uskutočnení finančnej transakcie držiteľom karty sa platobná karta pri spätnom pohybe zasekne, ešte pred vydaním hotovosti. Páchateľ, ktorý je zvyčajne nablízku, ubezpečí držiteľa o tom, že sa mu stalo pred chvíľou to isté a pre vrátenie karty stačí len zopakovať zadanie PIN kódu (ktorý si pri tom zapamätá). Samozrejme, ani po tejto operácii bankomat kartu nevydá a páchateľ „náhodou“ pozná telefónne číslo prevádzkovateľa bankomatu, na ktoré je potrebné nahlásiť problém (číslo je samozrejme falošné a obsluhuje ho páchateľov komplic). Páchateľ presvedčí obeť, aby na číslo zavolala. Prostredníctvom telefonického rozhovoru si jeho komplic u držiteľa karty opätovne overí základné údaje a PIN kód. Po odchode držiteľa karty páchateľ pomocou pinzety z bankomatu vyberie fóliu aj zaseknutú platobnú kartu a s použitím platného PIN kódu uskutoční nelegálny výber hotovosti.

Pozor si treba dávať aj pri platení kartou

Pozrite si tieto videá, aby ste videli, ako ľahko môže obsluha v reštaurácii zneužiť vašu kartu:
http://www.youtube.com/watch?v=Ns80IjFHyrg http://www.youtube.com/watch?v=U0w_ktMotlo

V prvom rade nedávajte svoju platobnú kartu do rúk nikomu inému, komu nedôverujete. Vždy ostaňte so svojou platobnou kartou a v podniku nikdy nevkladajte kartu do púzdra s účtom, radšej obsluhu poproste, aby priniesla prenosný POS terminál. Dávajte celý čas pozor, či s vašou kartou nenakladá inak, ako by mal (napríklad či si ňou neprechádza pri opasku alebo ju nedáva niekam pod pult). Takéto praktiky sú veľmi bežné... PIN kód zadávajte zásadne tak, aby ste si druhou rukou zakrývali tlačítka, poprípade obsluhu poproste aby sa otočila. V obchode sledujte celý proces platby a nedovoľte, aby predavač prešiel vašou kartou pod pultom.
Samozrejme, z hľadiska ochrany pred zneužitím karty obsluhou je najlepšie platiť v hotovosti...

Je skimming naozaj rozšírený?

Podľa niektorých štatistík patrí skimming na tretie miesto najbežnejšej formy odcudzenia platobnej karty, pričom za rok 2007 bolo evidovaných viac ako 700,000 prípadov len na území UK. Postihnutých je aj mnoho turistických destinácií. Ročne sú takto odcudzené desiatky miliárd korún a väčšina páchateľov nie je nikdy odhalená.

Stretneme sa s ním aj u nás?

V roku 2008 sa obeťami skimmingu stali zákazníci Slovenskej Sporiteľne, ktorých údaje o platobných kartách boli skopírované a následne bol z ich účtov vytiahnutý značný obnos peňazí v Taliansku. *„Zneužitých bolo niekoľko desiatok kariet,“* povedal hovorca Slovenskej sporiteľne Štefan Frimmer. Klientov „zradil“ koncom marca bankomat na rohu Záhradníckej ulice a Odborárskeho námestia, len kúsko od Justičného paláca.
V automate Slovenskej Sporiteľne v Martine bolo v roku 2008 objavené zariadenie na snímanie údajov z platobnej karty a skrytá kamera, ktorá nahrávala PIN kódy klientov.

Falošné čítacie zariadenie bolo tiež namontované na vstupných dverách k bankomatu v jednej z pobočiek ČSOB v Českej republike.

Zhrnutie – rady ako sa chrániť

- Nikomu neprezrádzajte svoje PIN-číslo, nepovedzte ho ani rodinným príslušníkom, zamestnancom banky a ani polícii. Zapamätajte si ho a nikdy si ho nezapisujte na bankovú platobnú kartu. Pokiaľ PIN-číslo zabudnete, požiadajte svoju banku o jeho znovuvytlačenie. Pri zadávaní PIN-čísla dbajte na to, aby nebolo prezradené.
- Ak sa vám podarí objaviť infikovaný bankomat, okamžite volajte políciu a nevzďaľujte sa od bankomatu. Zlodej je pravdepodobne na blízku a bude striehnuť na prvý moment, kedy bude môcť celé zariadenie zbaliť. Ak ste aj bankomat použili a zariadenie ste objavili až potom, neľakajte sa. Pokojne nahláste celú situáciu polícii a potom zablokujte svoju platobnú kartu na čísle, ktoré vám banka dala pri jej vydávaní. Zlodej aj pri použití ovládania na diaľku nestihne údaje z karty dopraviť svojim komplicom skôr, ako vy budete mať kartu zablokovanú. A ak je karta zablokovaná, bankomat ju zadrží a zlodejovi vznikne minimálne škoda.