ATM skimming напади и снимање на PIN-от

Прирачник за обука на корисниците на картички на Централна кооперативна банка АД Скопје

Што е ATM Card Skimming ?

- Метода која се користи од криминалците за собирање податоци од магнетната лента на задната страна од картичката
- Уредите кои се користат се скоро идентични со читачот за картички и најчесто се прикачуваат во близина или директно на фабрички инсталираниот читач на картички на АТМ-от
- ATM skimming е светски распространет проблем и се прави на сите видови банкомати

Како да забележите skimmer уред на АТМ-от ?

Проверувајте ги следните точки за можни сомнителни уреди

- Влезното место на читачот на картички
- Тастатурата за внес на податоци
- Копчиња за избор на опција од странита на екранот
- Областа околу звучникот
- Области на АТМ-от кои емитираат светлина

Што е снимање на PIN-от ?

- Стратешко поставување на камери или уреди за снимање на слики кои недозволено прават снимање на вашиот PIN
- Откако се снимени, електронските податоци се внесуваат на посебна (измамничка) картичка и снимениот PIN се злоупотребува за подигнување на средства од сметката
- Снимање на PIN-от е светски распространет проблем и се прави на сите видови банкомати

Skimming уреди – забележете ја разликата

Нормален изглед
- Светлоста од читачот на картички лесно се забележува
- Повеќето skimming уреди ќе ја блокираат светлоста од читачот на картички
- Овој детал најлесно открива поставеност на сомнителен уред

Skimming уред прикачен на АТМ-от
- Уредот е дизајниран да изгледа слично како и оригиналниот читач на картички
- нема светлост од читачот на картички и маската е забележливо различна

Типови на банкомати кои се користат во ЦКБ АД Скопје

NCR ATM

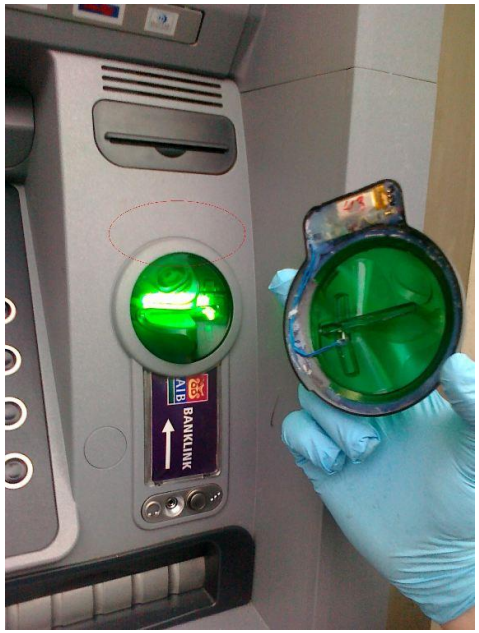
Wincor Nixdorf ATM

Skimming уред за NCR ATM

Изглед на skimming уред пред да биде поставен на АТМ

Skimming уред за NCR ATM

Skimming уред поставен на АТМ



Skimming уред за Wincor Nixdorf ATM

Skimming уред пред да биде поставен на АТМ

Skimming уред за Wincor Nixdorf ATM

Skimming уред поставен на АТМ

Уред за снимање на PIN

Изглед на тастатура за снимање на PIN

Уред за снимање на PIN

Уред прикачен на горниот дел од АТМ-от за снимање на PIN

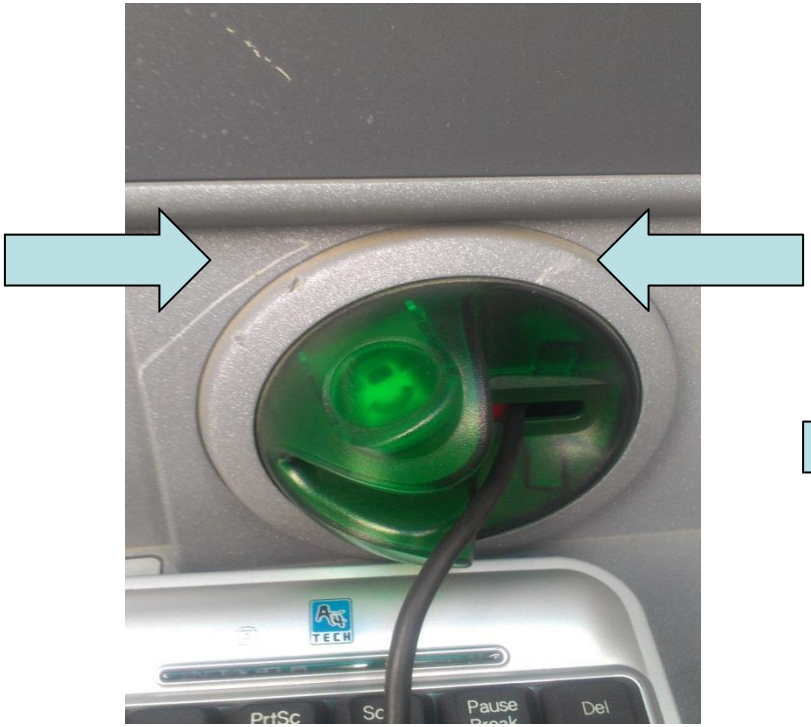
Уред за снимање на PIN

држач за брошури
прикачен на АТМ-от

камера на држачот
која го снима PIN-от

Знаци дека на АТМ-от е направен обид за поставување на skimming уред

Оштетување на читачот на картички



Оштетување на тастатурата

Факти за skimming уреди

- Skimming уредите се поставуваат на АТМ-ите во време на слаба фрекфенција на луѓе, рано наутро или доцна навечер
- Периодот во кој Skimming уредите се поставени на АТМ-ите обично е 24 часа
- За успешно крадење на податоци потребно е и двата уреда (skimmer& камера за снимање на PIN) да бидат поставени на АТМ-от
- Криминалците често се во близина на АТМ-от со цел брзо и незабележително одстранување на skimming уредите од АТМ-от по трансакција на клиентот

Како да го намалите ризикот ?

- Информирајте се за изгледот на АТМ-от и клучните точки – тастатура, читач на картичка, светлосни индикатори
- Пред подигнување на средства од АТМ-от, визуелно проверете го АТМ-от за можни поставени сомнителни уреди
- Проверете дали има дополнителна невообичаена опрема (држач за брошури, дополнителна маска или други делови)
- Секогаш покривајте ја тастатурата со слободната рака при внес на PIN-от
- Доколку забележите било каков сомнителен детал веднаш пријавете го во најблиската експозитура на Банката
- Бидете претпазливи, секогаш може да се намали ризикот од skimming