Студентка: Єлизавета Левенець
Керівник: Світлана Оліфірова

Скімінг - вид шахрайства з банківськими картами, при якому використовується скімер - інструмент для зчитування, наприклад, магнітної доріжки платіжної картки. При здійсненні даної шахрайської операції використовується комплекс скімінгових пристроїв:

Інструмент для зчитування магнітної доріжки платіжної картки є пристрій, що встановлюється на картоприймач банкомату або на картридер біля вхідних дверей в зону обслуговування клієнтів в приміщенні банку. Являє собою пристрій зчитує магнітною головкою, підсилювачем-перетворювачем, пам'яттю і перехідником для підключення до комп'ютера. Скімери можуть бути портативними, мініатюрними.

Мініатюрна відеокамера, яка встановлюється на банкомат і спрямовується на клавіатуру введення у вигляді козирка банкомату або сторонніх накладок, наприклад, рекламних матеріалів. За допомогою відеокамери відбувається спостереження за набором пін-коду в цілях його розкрадання.

Фальш-клавіатура, яка може використовуватися для розкрадання пін-коду карти замість міні відеокамери. Фальш-клавіатура встановлюється поверх штатної клавіатури банкомату таким чином, що при натисканні на її кнопки докладені зусилля передаються на кнопки справжньої клавіатури. Однак в момент натискання на кнопки відбувається реєстрація номерів кнопок і послідовність їх натискання.

Дані пристрою живляться від автономних джерел енергії - мініатюрних батарей електроживлення, і, для утруднення виявлення, як правило, виготовляються і маскуються під колір і форму банкомату.

Скімери можуть накопичувати вкрадену інформацію про пластикові картки, або дистанційно передавати її по радіоканалу зловмисникам, які знаходяться поблизу.

Шимінг, являє собою різновид скімінгу. В цьому випадку в картридер банкомату поміщається електронний пристрій (шимер), що дозволяє отримати інформацію про банківську карту. Товщина шимера - близько 0,2 мм. Зовнішнє визначення використання шимера вкрай утруднено. На цей час єдиним дієвим захистом від шимінгу є використання чипових пластикових карт.

Як розпізнати скімінг?

В першу чергу потрібно порівняти банкомат з його екранною заставкою:

Накладна клавіатура

Накладна клавіатура, вона може трішки більше випирати, ніж основна, тобто це накладочка зверху:

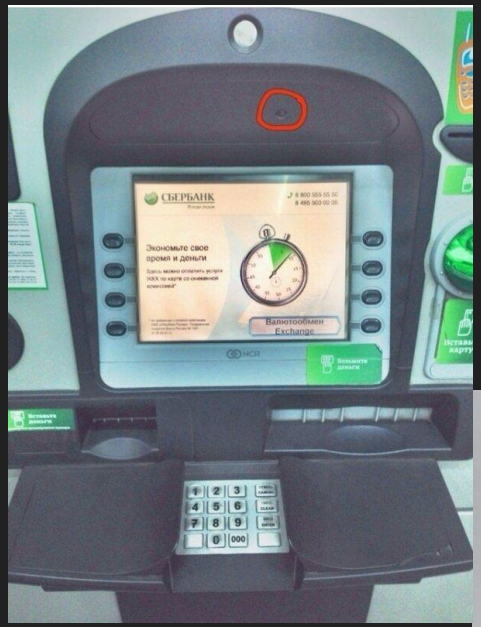
Картоприймач

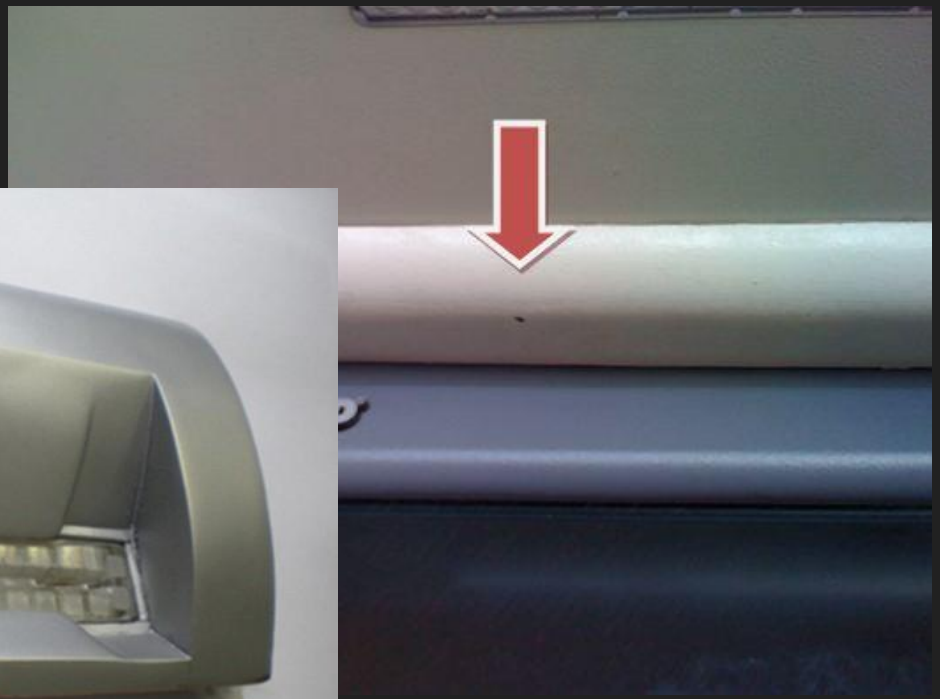
Поганий зовнішній вигляд

В більшості випадків після «модифікації» шахраями банкомату залишаються сліди, а саме різні вм’ятини, царапини, залишки клею, наліпки в місцях де їх не повинно бути.

Підозрілий банкомат

Відеокамера





Предмети поруч з банкоматом

Як вберегтися від скімінгу?

1. Уважно вивчайте зовнішній вигляд банкомата і схожість з картинкою на екрані.

2. Ніколи не пишіть PIN-код на платіжній картці і не зберігайте записаний PIN-код разом з платіжною карткою – це як залишити відкриту машину з ключами в замку запалювання. Вивчіть PIN-код напам'ять.

3. Ніколи і нікому не повідомляйте свій PIN-код. Його не має права вимагати у Вас ніхто: ані працівник банку, ані працівник правоохоронних органів.

4. Ніколи не передавайте платіжну картку (або її скановану копію) іншій особі. Чи маєте Ви гарантію, що особа, якій Ви довірили платіжну картку, теж уважно читала цей матеріал?

5. Ніколи й нікому не повідомляйте номер своєї платіжної картки.

6. Ніколи не залишайтеся бездіяльними при втраті або крадіжці платіжної картки! Негайно повідомте банку про цей випадок за телефоном Контакт-центру, номер якого рекомендуємо записати в мобільний телефон для оперативного блокування платіжної картки у випадку її втрати або крадіжки.

7. Ніколи не нехтуйте можливістю встановлювати ліміти на операції по платіжній картці. Якщо Ви не витрачаєте на добу більше тисячі гривень, навіщо встановлювати можливість витрачати більше?

8. Ніколи не дозволяйте допомагати Вам здійснювати операції по платіжній картці третім особам, не дозволяйте бачити платіжну картку та введення PIN-коду стороннім, хто стоїть у Вас за спиною.

9. Сплачуйте операції в торговельно-сервісній мережі (при розрахунку в магазинах / торгових точках / аптеках / ресторанах / АЗС / готелях та ін.) платіжною карткою лише власноруч, у крайньому випадку уважно стежте за діями касира / продавця.

10. Наполегливо рекомендуємо встановлення SMS-інформування щодо всіх операцій по Вашій платіжній картці на Ваш мобільний телефон.


ЦЕ СКІМІНГ?