Марков В.В., Гнусов Ю.В, Онищенко Ю.М.

Тренінгове заняття «Шахрайство з платіжними картками» (виявлення пристроїв для незаконного втручання в роботу банкоматів)

Фабула	Дії працівників поліції
17.05.2016 в 19:05 до чергової частини Жовтневого ВП ГНУП в Харківській області звернувся громадянин Грач О.М., який повідомив про те, що він став жертвою шахрайських дій – з його банківського рахунку (номер платіжної карти «5168 7555 1478 4567») зникли грошові кошти у сумі 6000 гривень. Грач О.М. повідомив, що 17.05.2016 о 17:30 він скористався банкоматом, що розташований за адресою: м. Харків, пр. Гагаріна, 25, для зняття готівки (сума – 200 гривень). О 18:30, 18:32, 18:34 на його мобільний телефон прийшло три SMS-повідомлення з інформацією про успішно здійснені перекази грошових коштів (у сумі по 2000 гривень кожний) на рахунок (банківську картку "4149 4978 5021 2318"). Зі слів Грача О.М. у вказаний час він перебував вдома, що можуть підтвердити сусіди по приватному будинку, та ніяких транзакцій не здійснював. О 18:35 Грач О.М. зателефонував на гарячу лінію банку та повідомив про подію, після чого його картку було заблоковано працівником фінансової установи.	1. Висувається версія про те, що громадянин Грач О.М. став жертвою шахрайських дій невстановлених осіб з його банківською платіжною карткою, здійснених зловмисниками за допомогою незаконно встановленого технічного обладнання на банкоматі. 2. Працівники поліції повинні провести зовнішній огляд банкомату, яким останній раз користувався гр. Грач О.М., з метою можливого виявлення на ньому пристроїв для несанкціонованого отримання реквізитів платіжних карток та подальшого незаконного отримання доступу до рахунку особи у банку (наприклад, скімер, накладна клавіатура, мініатюрна відеокамера для фіксації набору пін-коду картки користувачем). 3. Після огляду банкомату у разі виявлення незаконно встановлених пристроїв працівники поліції вживають заходи для документування (у тому числі шляхом застосування засобів фіксування інформації) фактів розташування пристроїв негласного зйому інформації на банкоматі та повідомляють про даний факт працівників територіального підрозділу Департаменту кіберполіції Національної поліції України.

Тренінгове заняття
«Шахрайство з платіжними картками»
(виявлення пристроїв для незаконного втручання в роботу банкоматів)

Мета заняття: курсанти повинні навчитися ідентифікувати пристрої, що використовуються для незаконного втручання в роботу банкоматів.

Місце проведення: ауд. № 111/5 (аудиторія з банкоматом).

Матеріально-технічне забезпечення:

- банкомат;
- комп'ютер;
- проектор;
- екран.

Фабула:

17.05.2016 в 19:05 до чергової частини Жовтневого ВП ГНУП в Харківській області звернувся громадянин Грач О.М., який повідомив про те, що він став жертвою шахрайських дій – з його банківського рахунку (номер платіжної карти "5168 7555 1478 4567") зникли грошові кошти у сумі 6000 гривень. Грач О.М. повідомив, що 17.05.2016 о 17:30 він скористався банкоматом, що розташований за адресою: м. Харків, пр. Гагаріна, 25, для зняття готівки (сума – 200 гривень). О 18:30, 18:32, 18:34 на його мобільний телефон прийшло три SMS-повідомлення з інформацією про успішно здійснені перекази грошових коштів (у сумі по 2000 гривень кожний) на рахунок (банківську картку "4149 4978 5021 2318"). Зі слів Грача О.М. у вказаний час він перебував вдома, що можуть підтвердити сусіди по приватному будинку, та ніяких транзакцій не здійснював. О 18:35 Грач О.М. зателефонував на гарячу лінію банку та повідомив про подію, після чого його картку було заблоковано працівником фінансової установи.

План заходів:

1. Висувається версія про те, що громадянин Грач О.М. став жертвою шахрайських дій невстановлених осіб з його банківською платіжною карткою, здійснених зловмисниками за допомогою незаконно встановленого технічного обладнання на банкоматі.

2. Працівники поліції повинні провести зовнішній огляд банкомату, яким останній раз користувався гр. Грач О.М., з метою можливого виявлення на ньому пристроїв для несанкціонованого отримання реквізитів платіжних карток та подальшого незаконного отримання доступу до рахунку особи у банку (наприклад, скімер, накладна клавіатура, мініатюрна відеокамера для фіксації набору пін-коду картки користувачем).

3. Після огляду банкомату у разі виявлення незаконно встановлених пристроїв працівники поліції вживають заходи для документування (у тому числі шляхом застосування засобів фіксування інформації) фактів розташування пристроїв негласного зйому інформації на банкоматі та

повідомляють про даний факт працівників територіального підрозділу Департаменту кіберполіції Національної поліції України.

План заняття

1. Ознайомлення курсантів із:

1.1. Загальними поняттями, використовуваними під час дистанційного банківського обслуговування.

1.2. Типами пластикових карток, їхніми ідентифікаційними реквізитами.

1.3. Типами та принципами дії банківського обладнання для дистанційного обслуговування (банкомати, платіжні термінали, POS-термінали).

1.4. Алгоритмами протиправних дій у сфері використання платіжних карток:

- фізичний скімінг;
- програмний скімінг;
- прямий диспенс;
- фальшивий банкомат;
- transaction reversal fraud;
- cash trapping;
- card trapping;
- використання підробленних карток (білого пластику);
- банкоматне шахрайство з використанням методів соціальної інженерії.

2. Набуття курсантами практичних навичок виявлення пристроїв для незаконного втручання в роботу банкоматів:

- скімерів;
- шимерів;
- накладок на диспансер банкомату;
- прихованих мініатюрних відеокамер;
- фальшивих клавіатур;
- пристроїв типу «Ліванська петля»).

3. Проведення з курсантами рольової гри "Реалізація алгоритму дій працівника поліції на місці події (під час факту виявлення пристроїв для незаконного втручання в роботу банкоматів)".

Хід заняття

1. Тренер проводить з курсантами рольові ігри з різними вихідними даними про отримання поліцейськими інформації про протиправні дії у сфері використання банківських платіжних карток або банківського обладнання.

Ігрові ситуації:

1) встановлення, знімання або виявлення на банкоматі пристрою для несанкціонованого доступу до платіжних даних;

2) налаштовування банкомату сторонніми особами через пін-клавіатуру;

3) отримання невідомими особами значних коштів без введення ними після кожного отримання грошей pin-коду;

4) банкомат не видає гроші з банківського рахунку клієнту;

5) фізична атака на банкомат;

6) несанкціонований вивіз банкомату з місця його стаціонарного встановлення.

Джерела, з яких поліцейські отримали інформацію про правопорушення:

1) від заявника;

2) від чергового по територіального підрозділу поліції;

3) самостійно виявили.

Заявники:

1) свідок;

2) жертва правопорушення;

3) представник банку.

2. Курсанти імітують отримання інформації про протиправні дії у сфері використання банківських платіжних карток або банківського обладнання.

3. Курсанти опитують заявника про те чому на його думку тут відбувалися протиправні дії у сфері використання банківських платіжних карток або банківського обладнання.

4. Курсанти в разі необхідності приховано оглядають місце скоєння злочину.

5. Курсанти забезпечують приховане спостереження за місцем скоєння злочину.

6. Курсанти імітують інформування чергової частини про факт вчинення протиправних дій у сфері використання банківських платіжних карток або банківського обладнання.

7. Курсанти забезпечують охорону місця події до прибуття слідчо-оперативної групи.

8. Курсанти намагаються виявити відеокамери, що могли зафіксувати осіб, які вчинили злочин або момент скоєння злочину.

9. Курсанти намагаються виявити свідків вчинення злочину.

Теоретична частина

Поліцейські при виявленні осіб, які причетні до втручання в роботу банкоматів або проводять операції з використанням підроблених платіжних карток повинні:

1. Ідентифікувати особу / осіб.

2. В ході особистого огляду звертати увагу та фіксувати:

1) пластикові картки:

– картки з реквізитами платіжних карток;

– дисконтні картки;

– пластикові заготовки карток без нанесення персоналізованої інформації;

2) пристрої, що можуть бути використані для скоєння протиправних

дій у сфері використання платіжних карток;

3) чеки, квитанції, документи, що підтверджують проведення операцій по картці та містять дані про операції;

4) інформаційні носії;

5) одяг та аксесуари одягу.

Практична частина

Необхідне знаряддя:

1) документи, що посвідчують особу:

– паспорт;

– водійське посвідчення;

2) банківські платіжні картки;

3) скімінгове обладнання, що поміщається у кишеню або сумку;

4) набір викруток;

5) клейка стрічка (скотч);

6) чеки від банкоматів про проведенні операцій та транзакції;

7) USB флеш-носії.

1. Тренер проводить з курсантами рольові ігри з різними вихідними даними про виявлення особи/осіб, які причетні до втручання в роботу банкоматів або проводять операції з використанням підроблених карток.

2. Курсанти зупиняють підозрілу особу та ідентифікують її.

3. Курсанти проводять поверхневий огляд особи та її речей.

4. Курсанти виявлять речі, що свідчать про причетність особи до несанкціонованого втручання у роботу банкоматів.