Конкурс
Защита прав потребителей
финансовых услуг

ТЕМОЦЕНТР

БАНКОВСКИЕ ПЛАТЕЖИ И КАРТЫ: ИГРА ПО ПРАВИЛАМ И БЕЗ

ОСНОВНЫЕ ВИДЫ МОШЕНИЧЕСТВА И СПОСОБЫ ЗАЩИТЫ

Основные вопросы:

1.Наиболее распространенные способы мошенничества в области пластиковых карт и различных дистанционных платежей

2.Принципы защиты от угроз, формирование безопасного финансового поведения и ответственного отношения к безопасности транзакций

3.Обсуждение конкретных случаев мошенничества

4.Рекомендации по уменьшению подверженности мошенничеству

5.Принципы работы по противодействию и выявлению мошенничества в части банковских карт и иных ЭСП

Как происходит карточная транзакция

1. Вы приходите с картой к банкомату, в магазин, оплачиваете на сайте в интернете, сообщаете данные карты в гостиницу, прикладываете к терминалу, пишете в банке заявление на перевод с карты.

2. Терминал/сайт/банкомат формирует запрос на осуществление авторизации и направляет банку-эквайреру, либо проводит платеж сам, без авторизации

3. При платеже с авторизацией банк-эквайрер направляет через платежную систему запрос банку-эмитенту: «можно ли оплатить картой и достаточно ли на ней средств для совершения покупки?»

4. Банк-эмитент одобряет транзакцию либо ее отклоняет. Если транзакция одобрена – с этого момента у банка-эмитента возникает обязательство

5. Банк-эквайрер дает разрешение торговой точке отпустить товар, выдать деньги в банкомате, осуществить перевод средств и.т.д.

6. **Затем, в период от нескольких часов до 30 дней с момента транзакции, банк-эквайрер направляет финансовое сообщение, на основании которого осуществляются расчеты между банками, и со счета клиента списываются средства. До этого момента сумма на счету блокируется**

Базовые качества жертв, используемые мошенниками

- **ГЛУПОСТЬ**
- **ЖАДНОСТЬ**
- **СТРАХ**

- **БЕЗОТВЕТСТВЕННОЕ ПОВЕДЕНИЕ**
- **ПРЕНЕБРЕЖЕНИЕ МЕРАМИ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ КАРТЫ ИЛИ ДБО**

Технологические предпосылки мошенничества в сфере карт, ДБО, мобильных платежей

Широкое распространение коммуникационных устройств среди населения, не подготовленного к противодействию мошенничеству, бесконтрольная продажа контрактов мобильной связи

Использование технических средств для осуществления платежных операций в автоматическом режиме без личного присутствия владельца средств для осуществления платежа или передачи денег другому лицу

Движение денежных средств на основе единых принципов и правил коммуникации и платежей

Недочеты в законодательстве о платежах и услугах связи, Недостаточность мероприятий противодействия мошенникам

Отсутствие единой федеральной системы мониторинга мошеннических транзакций и противодействия хищениям электронных денег

Особенности современных групп кибер-мошенников

1. Несколько участников группы имеют высшее образование и обладают навыками в области ИТ, психологии, знают приемы НЛП
2. Для хищения используются компьютеры, мобильные телефоны, современные средства коммуникации, карты, мобильные кошельки
3. Организация строится по распределённому принципу, в связи с чем практически невозможно вычислить всех участников группы
4. Задания передаются через анонимные сетевые сервисы или по СМС, деньги переводятся на карты преступников через цепочку посредников
5. Как правило, преступление совершается в несколько этапов, реализация которых может осуществляться участниками группы в различных странах
6. Существует значительное число каналов незаконной торговли похищенной финансовой информацией и обмена сведениями о действиях служб безопасности банков и правоохранительных органов.

Угрозы у банкомата

- **НАПАДЕНИЕ У БАНКОМАТА**
- **ЛИВАНСКАЯ ПЕТЛЯ**
- **ВИЛКА, (CASH TRAPPING и.т.д)**
- **СКИММИНГ**
- **ШИММИНГ**
- **СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ**

Нападение у банкомата:

- НЕПОДОБАЮЩЕЕ МЕСТО
- НОЧНОЕ ВРЕМЯ СУТОК
- ПОСТУПКИ, ПРОВОЦИРУЮЩЕЕ ГРАБЕЖ
- НЕВНИМАТЕЛЬНОСТЬ, БЕСПЕЧНОЕ ПОВЕДЕНИИЕ ДЕРЖАТЕЛЯ

ЧТО ДЕЛАТЬ ?

1. ОБРАТИТЬСЯ В ПОЛИЦИЮ
2. ЗАБЛОКИРОВАТЬ КАРТУ, ЕСЛИ ЕЕ ПОХИТИЛИ ВМЕСТЕ С ДЕНЬГАМИ

Нападение у банкомата:

- **НЕВНИМАТЕЛЬНОСТЬ, БЕСПЕЧНОЕ ПОВЕДЕНИИЕ ДЕРЖАТЕЛЯ**
- **ПРОВЕДЕНИЕ ОПЕРАЦИИ ЕСЛИ РЯДОМ НАХОДЯТСЯ КАКИЕ-ТО ЛЮДИ.**

КАК ИЗБЕЖАТЬ ?

1. **ОСМОТРЕТЬСЯ ПЕРЕД СНЯТИЕМ ДЕНЕГ**
2. **ИСПОЛЬЗОВАТЬ ЗЕРКАЛА НА БАНКОМАТЕ, ЧТОБЫ ВИДЕТЬ, ЧТО СЗАДИ ВАС**
3. **ПРИ СНЯТИИ КРУПНОЙ СУММЫ ДОГОВОРИТЬСЯ О СОПРОВОЖДЕНИИ**

Ливанская петля:

- КАРТА «ЗАСТРЯЛА»
- РЯДОМ – ДОБРОЖЕЛАТЕЛЬНЫЙ ПОМОЩНИК, РЕКОМЕНДУЕТ ВВЕСТИ ПИН
- УХОД ОТ БАНКОМАТА «ЗА ПОМОЩЬЮ»
- КАРТА УКРАДЕНА, СРЕДСТВА ПОХИЩЕНЫ

ЧТО ДЕЛАТЬ ?

1. НЕ ПРИНИМАТЬ НИКАКОЙ ПОСТОРОННЕЙ ПОМОЩИ У БАНКОМАТА
2. СВЯЗАТЬСЯ С БАНКОМ – ВЛАДЕЛЬЦЕМ БАНКОМАТА ИЛИ ПОЛИЦИЕЙ
3. ДЕЙСТВОВАТЬ ПО ОБСТОЯТЕЛЬСТВАМ
4. СВЯЗАТЬСЯ С БАНКОМ ЭМИТЕНТОМ КАРТЫ
5. ЕСЛИ КАРТУ ДОСТАТЬ НЕ УДАЛОСЬ – БЛОКИРОВАТЬ

CASH TRAPPING:

- **БАНКОМАТ «ПРОШУРШАЛ», СРЕДСТВА СПИСАЛИСЬ С КАРТЫ, НО НЕ ПОЯВИЛИСЬ ИЗ ДИСПЕНСЕРА**
- **ИНОГДА ИЗ ДИСПЕНСЕРА МОГУТ ВЫСТУПАТЬ НЕШТАТНЫЕ ПРЕДМЕТЫ (ВЕРЕВКА, «ЖЕЛЕЗКА»)**
- **ДВА ВАРИАНТА РАБОТЫ БАНКОМАТА ПОСЛЕ ИНЦИДЕНТА:**
  - **перешёл в режим ожидания**
  - **завис или пишет о неисправности.**

ЧТО ДЕЛАТЬ?

1. **ПОПЫТАТЬСЯ ПОЛУЧИТЬ ПОВТОРНО НЕБОЛЬШУЮ СУММУ**
2. **СВЯЗАТЬСЯ С БАНКОМ ЭМИТЕНТОМ КАРТЫ**
3. **СВЯЗАТЬСЯ С БАНКОМ – ВЛАДЕЛЬЦЕМ БАНКОМАТА ИЛИ ПОЛИЦИЕЙ**
4. **ДЕЙСТВОВАТЬ ПО ОБСТОЯТЕЛЬСТВАМ**
5. **ПРИ НЕОБХОДИМОСТИ – БЛОКИРОВАТЬ КАРТУ**

Скимминг: Схема мошенничества

Установка на банкомат или входную группу зоны расположения банкоматов электронного устройства для копирования данных магнитной полосы карты, получения сведений о ПИН коде и сохранения их в памяти устройства для дальнейшего использования мошенниками либо передача мошенникам по радиоканалу в режиме online.

Изготовление поддельной карты с магнитной полосой, аналогичной полосе оригинальной карты.

Использование поддельной карты и ПИН кода для проведения операций снятия наличных денежных средств или покупок легкореализуемых товаров в магазинах (электроника, телефоны, заправка, дорогая парфюмерия, фишки казино и др.)

МЕСТА УСТАНОВКИ:

- **КАРДРИДЕР**
- **ИНОГДА – НА ЗАМОК ДЛЯ ВХОДА В ЗОНУ**
- **ВНУТРЬ КАРДРИДЕРА**
- **ВНУТРИ БАНКОМАТА НА КАРДРИДЕР**
- **КАМЕРА – В ЛЮБОМ МЕСТЕ, ОТКУДА ВИДНА КЛАВИАТУРА, СВЕРХУ, СБОКУ, НА РАЗЛИЧНЫХ «РЕКЛАМНЫХ» НАКЛЕЙКАХ, РУЧКАХ и т.д.**

ЧТО ДЕЛАТЬ ?

1. **ПОЛЬЗОВАТЬСЯ БАНКОМАТОМ В ОТДЕЛЕНИИ БАНКА ИЛИ В КРУПНОМ ТОРГОВОМ ЦЕНТРЕ**
2. **ОСМАТРИВАТЬ БАНКОМАТ ПЕРЕД ВСТАВКОЙ КАРТЫ**
3. **ЕСЛИ ЕСТЬ СОМНЕНИЯ – НЕ ИСПОЛЬЗОВАТЬ.**

ФИШИНГ

- SMS ФИШИНГ
- E-MAIL РАССЫЛКИ
- ФАЛЬШИВЫЕ САЙТЫ
- «НА ГРОШ ПЯТАКОВ»
- «БЫТОВЫЕ» ЗВОНКИ
- СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

SMS, E-Mail-ФИШИНГ: схема мошенничества

Мошенники используют широковещательные рассылки, зачастую от имени Банка России, E-mail, SMS-сообщений следующего содержания:

Ваша карта заблокирована, информация по телефону (903) 11111111

По Вашей карте запланирован платёж на сумму 33500 рублей. Для отмены позвоните по телефону (903) 11111111

Вам поступил платёж на сумму 5768 фунтов стерлингов. Подтвердите получение, иначе платеж будет возвращён отправителю. Телефон для справок (903) 11111111

Поздравляем! Вы выиграли компьютер! Информация (800) 11111111

Цель сообщения - инициировать звонок держателя карты мошенникам. Во время звонка клиента убеждают подойти к банкомату и выполнить ряд процедур либо выясняют конфиденциальную информацию о карте, системе ДБО, кодовые слова …..

В результате клиент сам переводит денежные средства на карту или счет мобильного телефона мошенников, либо сообщает все данные карты, SMS пароли, кодовые слова затем мошенники переводят и обналичивают полученные средства.

«БЫТОВЫЕ ЗВОНКИ»:

Мошенники используют украденные базы данных с информацией об адресах, номерах телефонов, истории болезни в поликлинике…

Мошенники звонят на домашний телефон и сообщают о некотором событии (пересчете оплаты, изменении размера пенсии, выплатах, обходе дежурного врача, визите работника собеса, сборе информации о ветеранах труда, акции для пенсионеров, серьезном диагнозе на основании последних анализов.

Методами социальной инженерии побуждают жертву перевести средства либо впустить в квартиру «представителя» для общения.

Жертва переводит средства на счет мобильного телефона либо карту мошенников, для «подтверждения кода» или «участия в социальной программе» либо приобретают бесполезные предметы по завышенным ценам, либо подвергается ограблению в квартире.

Цель – Путем сообщения якобы «важной» информации добиться от жертвы исполнения инструкций мошенников либо допустить в квартиру.

ЗАМЕНА SIM КАРТЫ:

Мошенники используют недостатки в системе безопасности мобильных операторов и служб ДБО банков:

Методами фишинга (социальной инженерии) во время разговора с гражданином получают персональные данные (серия, номер паспорта, номер мобильного телефона), или через троянские программы проникают на домашний компьютер и находят всю информацию там, включая логин и пароль для входа в интернет банк

Изготавливают поддельные документы (паспорт, водительское удостоверение, нотариальная доверенность)

Получают в отделении оператора мобильной связи дубликат SIM карты, вставляют (обычно ночью) карту в свой телефон, после чего телефон законного владельца перестает работать, а мошенники получают все SMS направленные владельцу, в том числе банковские

Цель – Получить доступ к данным мобильного телефона либо к интернет банку и украсть деньги со счета в банке, пластиковой карты, счета мобильного телефона.

Кража средств через Интернет-Банк

(в т.ч. при наличии двухфакторной аутентификации)

Схема мошенничества более подробно:

1. Внедрение на компьютер жертвы вредоносной троянской программы либо манипулирование по телефону методами социальной инженерии
2. Получение информации о персональных данных, номерах счетов и карт.
3. Получение дубликата SIM карты в офисе оператора по поддельному паспорту, водительскому удостоверению, нотариальной доверенности.
4. Мониторинг финансовых потоков жертвы, выбор момента совершения преступления
5. Использование дубликата SIM карты в телефоне мошенников, перехват сообщений.
6. Хищение средств и перевод их на банковские счета, карты, счета мобильных телефонов или электронные кошельки, контролируемые мошенниками
7. Снятие наличных денежных средств либо покупка товаров и услуг для последующей перепродажи.

КАК ИЗБЕЖАТЬ ?

1. Не открывайте неизвестные вложения в письмах

Если Вы получили электронное письмо от подозрительного отправителя или получили от знакомого, но не договаривались об этом, или у Вас есть подозрения относительно письма и его вложений, в этом случае не открывайте вложенные файлы. Документы, которые на первый взгляд выглядят вполне безобидно (например, документ Word) могут содержать скрытые вредоносные программы. Даже простая фотография может оказаться опасной.

2. Не нажимайте, не подумав, на короткие ссылки

Если Вы используете Twitter или другой аналогичный сервис, то часто открываете ссылки, такие как bit.ly, известный ow.ly от Hootsuite или goo.gl от Google. Обычно, они не представляют какой-либо опасности для Вас, т.к. ведут на чей-либо блог или онлайн-ежедневник, но некоторые ссылки не являются такими безобидными, как может показаться, поэтому внимательно посмотрите на ссылку перед тем, как ее открыть, она может немного отличаться от привычных Вам.

КАК ИЗБЕЖАТЬ ?

3. Осмотрительно используйте публичный WI-FI

Интернет наполнен информацией об опасности использования публичных Wi-Fi сетей, например в кафе, гостинице, аэропорту или в библиотеке. Путем подмены Hot Spot или другими способами мошенники могут контролировать Ваш трафик. Не передавайте конфиденциальную информацию (пароли, банковские данные…) по возможности, используйте виртуальные частные сети (VPN), подключайтесь только к тем сайтам, которые используют безопасный протокол (это можно увидеть по наличию https в начале адреса сайта в адресной строке браузера).

4. Устанавливайте обновления безопасности

Если Ваша операционная система сообщает Вам, что необходимо что-то установить или обновить, то Вам следует обратить на это Ваше внимание и сделать это. В большинстве случаев, обновления связаны с внедрением мер безопасности для устранения недавно обнаруженных уязвимостей, которые могут быть использованы кибер-преступниками. Аналогично и в случае с Вашем сотовым телефоном: всегда используйте последнюю доступную версию Android или iOS и будьте в курсе, какие приложения у Вас установлены.

КАК ИЗБЕЖАТЬ ?

5. Используйте разные пароли для различных аккаунтов

Если кто-нибудь узнает или подберет Ваш пароль, то он сможет подключиться к другим Вашим аккаунтам. Кроме того, любая атака на корпоративные базы данных (что также становится распространенным явлением) может осуществляться с Вашими регистрационными данными.

6. Обязательно установите и обновляйте антивирус

Хорошая антивирусная программа – это самый лучший барьер, который Вы можете установить между Вашим компьютером и кибер-преступниками. Новые уязвимости, различные способы взлома Вашей личной информации, способы перехвата Вашего банковского счета – все это обнаруживается ежедневно.

7. Создавайте и обновляйте резервные копии документов

Создание резервных копий Ваших файлов происходит намного проще, чем это кажется со стороны, но если Вам лень даже думать об этом, имейте в виду, что есть достаточно много инструментов, которые могут автоматизировать решение данного вопроса, а в случае, например, появления на Вашем устройстве трояна – шифровальщика, наличие копии данных спасет Ваши нервы и деньги.

КАК ИЗБЕЖАТЬ ?

8. Обращайте внимание на сообщения браузера о безопасности

Когда Вы перемещаетесь по сайтам, Вы склонны действовать на автопилоте и часто игнорируете любые предупреждения, которые попадаются на глаза. Если, например, Chrome говорит, что сайт не безопасен, или Firefox запрашивает подтверждение перед скачиванием файла, не стоит автоматически давать разрешение, даже не задумываясь. Это – наиболее простой путь к проникновению вредоносных программ на Ваш компьютер.

9. С осторожностью публикуйте в социальных сетях персональную информацию

Особенно это касается тех случаев, когда Вы отправляетесь в отпуск или надолго покидаете квартиру, о чем подробно сообщаете в Facebook или Twitter. Хотя это актуально и для тех случаев, когда Вы сообщаете Ваше местоположение, совершенно не думая о том, что кто-то может воспользоваться этой информацией со злыми намерениями. Вся информация, которую Вы публикуете в социальных сетях, в конечном итоге может оказаться в руках мошенников.

КАК ИЗБЕЖАТЬ ?

10. Скачивайте только необходимые приложения и из известных источников

Вредоносные программы, разработанные для мобильных устройств, распространяются все шире, и одна из главных опасностей – это скачивание приложений вне Google Play и Apple Store. Официальные магазины предпринимают определенные меры для предотвращения распространения вредоносных программ (хотя и не всегда успешно), и Вы можете проверить отзывы других пользователей прежде, чем решите установить приложение или если Вы заметили что-то подозрительное. Если Вы скачиваете приложение с неофициального сайта и устанавливаете его на Ваше устройство, вероятность того, что приложение может содержать вредоносные программы, значительно возрастает.

11. С осторожностью подходите к любым финансовым сервисам, требующим ввода данных Вашей карты, Вашего счета, персональных данных, адресов, телефонов, особенно, если это связано с каким-то выигрышем, промо – акциями и т.д.

Простые правила безопасности:

- ☑ При любой операции с картой или с денежными средствами продумывать свои действия и учитывать возможные зловредные действия мошенников.
- ☑ Использовать только банкоматы, установленные в безопасных местах.
- ☑ Внимательно относиться к компьютерной безопасности, установить на компьютер антивирус, никогда не открывать файлы из незнакомых источников, никогда не открывать ссылки, присланные по электронной почте, не убедившись, что ссылка прислана Вашим знакомым либо сервисом, к которому Вы обращались.
- ☑ Не оставлять карту без присмотра, не передавать ее никому, никому и никогда не сообщать ПИН код, одноразовые пароли и другую информацию, пришедшую из банка по СМС **СОТРУДНИК БАНКА НИКОГДА НЕ МОЖЕТ ЗАПРОСИТЬ НОМЕР КАРТЫ, ПИН КОД, ПАРОЛИ, ПРИШЕДШИЕ ПО СМС.**
- ☑ **При любой проблеме с картой, сомнениях, подозрении о компрометации карты, срочно связаться с Банком ИСКЛЮЧИТЕЛЬНО по телефонам, указанным на обороте карты или на сайте Банка.**

Организации, ответственные за защиту прав плательщика

Служба по защите прав потребителей финансовых услуг
и миноритарных акционеров
Банка России http://www.cbr.ru/ электронная почта: mailto:fps@cbr.ru

Федеральная антимонопольная служба

http://www.fas.gov.ru

Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор)

http://rospotrebnadzor.ru

Банк России

www.cbr.ru

http://www.pandasecurity.com - Антивирус