Банк России

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ: КАК НЕ ПОТЕРЯТЬ СВОИ ДЕНЬГИ

Ибрагимов Дмитрий Андреевич

Заместитель начальника
Отдела технической защиты информации
ГУ Банка России по ЦФО

2019 г.

Актуальность

В Курской области по фактам несанкционированного списания денежных средств с банковских карт за период с января по апрель 2019 года по направлению мошенничества органами полиции зарегистрировано более 700 преступлений, из них краж (ст. 158 УК РФ) с использованием информационных технологий – более 150 преступлений.

Характерный пример:

15 апреля 2019 года в дежурную часть территориального отдела полиции обратилась гражданка Ф. (01.01.1940 года рождения, зарегистрирована по адресу: Курская область, …..) которая сообщила следующее: 27 марта 2019 года ей позвонил некий гражданин А. (телефонный номер 8-9ХХ-ХХХ-ХХ-ХХ) и представился якобы работником подразделения АО «ХХХ БАНК". Далее гражданин А. сообщил Ф., что *"... по причине сбоя компьютера у 60 клиентов банка сняты денежные средства со счетов, конкретно у Ф. - 4890 рублей, но он может помочь вернуть деньги, при этом попросил продиктовать номер имеющейся банковской карты и другие ее реквизиты...*"

Ф., не подозревая обмана, сообщила А. реквизиты банковской карты ПАО ХХХбанк (ХХХХ ХХХХ ХХХХ 3773), после чего с указанной карты были списаны 9790 рублей.

В настоящее время сотрудниками полиции в рамках возбужденного уголовного дела по ч.3 ст.158 УК РФ (кража) проводят необходимые оперативно-следственные действия, направленные на установления и задержание лиц, совершивших указанное выше преступление.

Темы для рассмотрения

- Доверие к информации
- Безопасное общение в сети
- Техническая безопасность
- Безопасность платежей

Банк России

ДОВЕРИЕ К ИНФОРМАЦИИ И ОБЩЕНИЕ В СЕТИ

Доверие к информации

Информационный взрыв

Для просмотра видео, передаваемого по миру в секунду, понадобится 5 лет.

Информационная диета

К чему может привести переизбыток информации?

Безопасное общение в сети

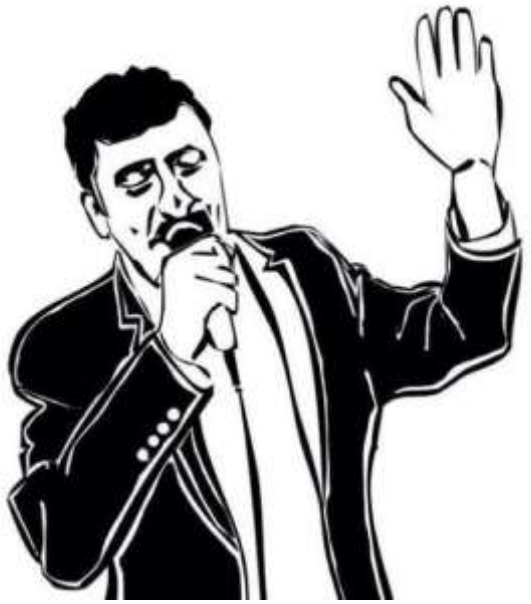
Какие правила безопасной коммуникации необходимо соблюдать в информационном пространстве?

ПРАВИЛА

Безопасное общение в сети

Запомните:

1. Все, что вы пишете, загружаете, пересылаете с помощью глобальной сети Интернет, **навсегда** останется в сети Интернет.
2. После публикации в Интернете текста или фотографии их невозможно контролировать.



А последствия?

Банк России

ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ

Техническая безопасность

1. Смартфон
2. Телефон
3. Планшет
4. Компьютер

А еще банкоматы, платежные и POS- терминалы. WiFi-роутеры, IoT-устройства и еще многое…

Задачи преступников

Получить контроль над:

- **Идентификационной информацией** — **Логин, пароль**
- **Каналом связи** — **WiFi, провода**
- **Устройством для управления** — **Телефон, компьютер, ATM**
- **ПО и ключевой информацией** — **ДБО, SteamOS**

Цели мошенников

Информация о деньгах

Информация о личности

Доступ к:

Банковским картам

Мобильному телефону

Компьютеру

Личным аккаунтам

Многообразие средств, используемых преступниками


Скиммер


Видеокамера


Фальшивый банкомат


Фемтосота


Черви

Блокировщики

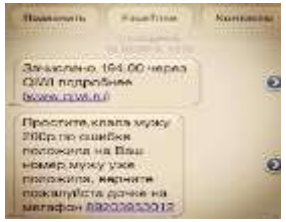

Сниффер

Спуфинг


Собирание мусора


«Флешка-подкидыш»

Фишинг


«Кража личности»

Распространенные каналы заражения вредоносным ПО

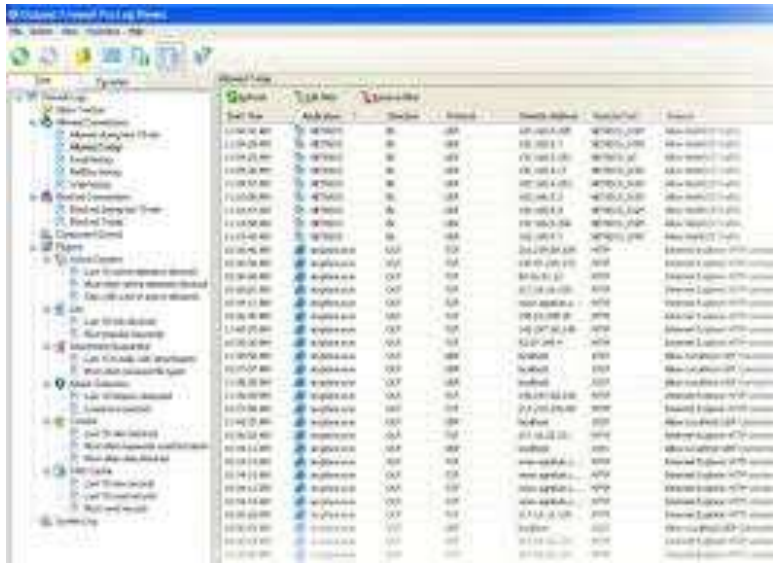
- Отчуждаемые носители информации (компакт-диски, дискеты и flash-накопители, мобильные телефоны и плееры и т. д.)
- Файлы из Интернета
- Программное обеспечение для мгновенного обмена сообщениями (используется в том числе для прямой передачи файлов).

Банк России

СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

Технические аспекты

Антивирусные средства



Межсетевые экраны

Технические аспекты

Шифрование и ЭЦП

Обновление ПО

Техническая безопасность

Правила безопасности

1. Регулярно обновляйте операционную систему и программы.
2. Используйте только лицензионные программы и данные, полученные из надежных источников.
3. Используйте антивирусную программу, которая постоянно обновляет свои базы, и регулярно проверяйте компьютер на наличие вирусов.
4. Создавайте резервные копии важных файлов, например на отдельном usb-накопителе.
5. Не используйте слишком простые пароли, которые можно легко угадать (даты рождения, номера телефонов и т. п.) и одинаковые пароли для разных систем.
6. При пользовании Интернетом на чужом устройстве не сохраняйте пароли и не забывайте выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы.
7. Не используйте публичные сети для передачи конфиденциальной информации

Банк России

БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ ПЛАТЕЖНЫХ КАРТ

Защита платежных карт

- CVV2 (Card Verification Value 2) трехзначный код проверки подлинности карты Visa
- CVC2 (Card Validation Code 2) аналогичный код для MasterCard

- Банки после 1 июля 2015 г. обязаны выдавать карты только с микропроцессором (чипом). Данные таких карт невозможно скопировать, что существенно затрудняет задачу скиммеров.

Защита платежных карт

Бесконтактные системы платежей основываются на Стандарте ISO/IEC 14443, описывающем частотный диапазон, метод модуляции и протокол обмена бесконтактных пассивных карт (RFID) ближнего радиуса действия (до 10 см) на магнитосвязанных индуктивностях.

Фишинг

Вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей

Пример № 1

*Звонок из банка с просьбой о погашении задолженности по кредиту. Абонент предсказуемо отрицает наличие задолженности и кредита, тогда «представители банка» просят его уточнить данные своей карты — **номер**, **PIN-код** и **дату выдачи**, чтобы «больше не беспокоить по этому поводу».*

Пример № 2

*Рассылка электронного письма, в котором от имени одного из крупных розничных банков сообщается о якобы последних новациях в его системе безопасности. Для отвода глаз запрашиваются некоторые сведения (вплоть до потребительских предпочтений), но самое главное — **номер карты** и **PIN-код** (еще могут попросить ответить на «контрольный вопрос»). К письму прикрепляется ссылка, якобы ведущая на сайт банка-эмитента карты. Но этот сайт — подделка, имитирующая логотип и дизайн сайта банка, которым пользуется выбранный мошенниками клиент.*

Пример № 3

Злоумышленники по электронной почте или на аккаунт в социальной сети присылают программный код, который рекомендуют выполнить, либо ссылку, по которой они предлагают перейти. Это делается под предлогом получения какой-нибудь интригующей или эксклюзивной информации.

На самом деле это фишинговая программа, скачивающая с вашего компьютера и пересылающая преступникам системные файлы, например ***cookies,*** *которые отражают маршрут заходов выбранной ими жертвы в различные сервисы.*

Вправе ли владелец платежной карты добровольно передать ее другому лицу?

*В отличие от находящихся на карточном счете средств сама карта является собственностью банка, а не клиента. Пользоваться ей может только тот человек, чьи фамилия и имя указаны на карте. Передача карты другим лицам и сообщение им **PIN-кода** — это нарушение порядка использования электронных средств платежа, устанавливаемого банками-эмитентами и международными платежными системами.*

Какие еще существуют механизмы защиты при совершении покупок через Интернет?

Двухфакторная аутентификация предполагает поэтапный доступ к онлайн-банку: сначала пользователь с компьютера вводит логин и пароль, затем для подтверждения входа в систему и проведения операций вводит дополнительные одноразовые коды. Самым популярным является отправка sms-сообщения с одноразовым паролем.

Подведем итоги

- Не пользуйтесь сомнительными устройствами
- Не реагируйте на провокации и соблюдайте спокойствие
- Не используйте публичные сети для передачи конфиденциальной информации
- При поступлении сообщений об операциях, которые вы не совершали, свяжитесь с банком, но только по официальным телефонам
- Не используйте один пароль на все системы
- Не посещайте сомнительные сайты, не совмещайте серфинг и работу с конфиденциальной информацией
- Не публикуйте в Интернете свои точные данные и их взаимосвязь

Банк России

СПАСИБО
ЗА ВНИМАНИЕ

Контакт-центр Банка России:
8 800 300-30-00