СТРАТЕГИЯ ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ
В РОССИЙСКОЙ ФЕДЕРАЦИИ НА 2017-2023 ГОДЫ

ФИНАНСОВОЕ КОНСУЛЬТИРОВАНИЕ

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Тема 8.3. Безопасность банковских карт и средств на банковских счетах

Дистанционное банковское обслуживание (ДБО) – общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом (т.е. без его визита в банк), чаще всего с использованием компьютерных и телефонных сетей.

Виды ДБО:

- **мобильный банкинг** – зачастую программа – клиент, устанавливаемая на personal digital assistant (pda – смартфон, планшет) устройство клиента. преимущество – удобство использования
- телефонный банкинг, sms – банкинг
- обслуживание с использованием банкоматов и платежных терминалов

Почему хищения возможны? Мы выделили **следующие факторы:**

- незащищенность компьютеров от современных вирусов (антивирусное программное обеспечение не эффективно)
- массовые заражения крупнейших легальных сайтов вирусами
- возможность удаленно управлять зараженным компьютером через сеть интернет
- низкая компьютерная грамотность

На рисунке (Рисунок 1) вы видите процесс хищения.

Рисунок 1. Процесс хищения

Вам представлен **пример схемы мошенничества,** это:

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.

Также представлен пример sms, e-mail-фишинга. Мошенники используют широковещательные рассылки, зачастую от имени банка россии, e-mail, sms-сообщений (Рисунок 2).

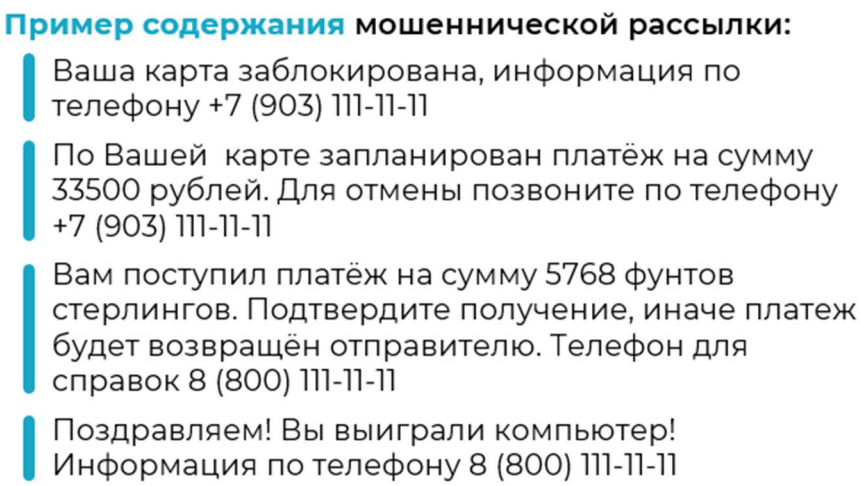

Рисунок 2. Пример содержания мошеннической рассылки.

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.

Ниже перечислены **некоторые способы защиты:**

- используйте сложные пароли
- никому не передавайте данные для входа в систему, в т.ч. сотрудникам банка
- перед вводом кода подтверждения операции из sms всегда проверяйте параметры операции, содержащиеся в сообщении
- установите и настройте антивирусное программное обеспечение
- подключите смс-информирование об операциях по счету
- при подозрении, что ваши данные для входа в систему стали известны третьим лицам, утере телефона устройства, которое вы используете для подтверждения операций в системе или обнаружении несанкционированных операций в системе, незамедлительно обратитесь в банк
- установите лимиты

Угрозы при использовании банковских карт

Физические:

- хищение банкомата: ручные приспособления, механизмы, техника.
- взлом банкомата: разрезание – болгарка, газосварка;
- высверливание замка (ригеля и т.п.); взрыв газообразной смеси.
- вандализм: монитор, ридер, диспенсер, фальшпанель.

Интеллектуальные:

- скимминг
- фальшивый банкомат
- траппинг (захват карты или наличных)
- кибератаки (вредоносное по, др.)
- получение наличных денежных средств по поддельным, утраченным картам

Угрозы нападения у банкомата:

- неподобающее место
- ночное время суток
- поступки, провоцирующее грабеж

Что делать ?

- обратиться в полицию
- заблокировать карту, если ее похитили вместе с деньгами

Также причиной нападения могут служить:

- невнимательность, беспечное поведение держателя
- проведение операции если рядом находятся какие-то люди.

Как избежать ?

- осмотреться перед снятием денег
- использовать зеркала на банкомате, чтобы видеть, что сзади вас
- при снятии крупной суммы договориться о сопровождении

Самая распространенная схему мошенничества – **бытовые звонки.**

Как правило, **мошенники используют украденные базы данных** с информацией об адресах, номерах телефонов, истории болезни в поликлинике и т.д.

Обычно **мошенники звонят на домашний телефон** и сообщают о некотором событии (пересчете оплаты, изменении размера пенсии, выплатах, обходе дежурного врача и т.д.

Затем методами социальной инженерии п**обуждают жертву перевести средства.**

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.

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

Далее мы рассмотрим **основные меры безопасности:**

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

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.

4. 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.

5. Обязательно установите и обновляйте антивирус

Хорошая антивирусная программа – это лучший барьер, который вы можете установить между вашим компьютером и кибер-преступниками.

7. Создавайте и обновляйте резервные копии документов:

- 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.

8. С осторожностью публикуйте в социальных сетях персональную информацию

9. Скачивайте только необходимые предложения 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.

10. 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

Запомните следующие правила:

- при любой операции с картой или с денежными средствами продумывайте свои действия и учитывайте возможные зловредные действия мошенников;
- используйте только банкоматы, установленные в безопасных местах;
- внимательно относитесь к компьютерной безопасности, установите на компьютер антивирус, никогда не открывайте файлы из незнакомых источников, никогда не открывайте ссылки, присланные по электронной почте, не убедившись, что ссылка прислана вашим знакомым либо сервисом, к которому вы обращались;
- не оставляйте карту без присмотра, не передавайте 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 свяжитесь с банком исключительно по телефонам, указанным на обороте карты или на сайте банка.

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ