

Модуль 8. Финансовая безопасность и мошенничество.

Тема 8.4. Схемы мошенничества с участием физических лиц и предпринимателей

Интернет-мошенничество на доверии – это самая распространенная в настоящее время схема мошенничества, которая может выглядеть следующим образом:

1. На телефонный номер держателя карты, разместившего в газете или на сайте публичное объявление о продаже того или иного имущества, поступает звонок от якобы потенциальных покупателей с целью приобрести данное имущество. После чего «потенциальный покупатель» предлагает удобную форму оплаты в виде пополнения банковской карты, для чего просит сообщить ему такие данные банковской карты, как номер карты, срок действия, проверочный код, а также дополнительный секретный код, направляемый банком в SMS-сообщении на мобильный телефон клиента при совершении клиентом операции в сети Интернет. Получив данную информацию, «потенциальный покупатель» совершает не операцию пополнения карточного счета клиента, а операцию по переводу/списанию денежных средств в сети Интернет с карты держателя, например, на свой электронный кошелек.
2. Мошенники представляются службой безопасности банка и сообщают клиенту о подозрительной операции по его карте и о возможности вернуть якобы списанные с карты деньги. Либо сообщают о сбое в системе банка и необходимости заблокировать карту. Для решения проблемы мошенники просят сообщить данные карты, пароли от мобильного банка. При этом злоумышленники с помощью современных технологий используют подмену номеров телефонов под официальные номера банка, тем самым усыпляя бдительность клиента.
3. Мошенники сообщают, что с банковской картой клиента или мобильным приложением произошел некий инцидент, и убеждают установить приложения, якобы защищающие денежные средства.

Такие приложения могут оказаться программами удаленного доступа и управления устройством клиента: TeamViewer, AnyDesk или их аналоги. После установки такой программы и получения ID и кодов доступа мошенники подключаются к устройству жертвы и могут управлять им, просматривать любую информацию, выполнять операции через мобильный банк.

4. Мошенники активно используют тему коронавирусной инфекции и состояние обеспокоенности людей для хищения денежных средств. Злоумышленники могут представиться работниками Пенсионного фонда, Роспотребнадзора и других государственных или социальных организаций, сообщить о положенной социальной выплате или материальной помощи, тем самым вынуждая предоставить информацию о карте, кодах, паролях из смс, персональных данных, либо совершить какие-либо действия для получения выплат.

Оставление карты в банкомате – в случае применения этой новой схемы мошенники якобы случайно забывают карту в банкомате и просят ее изъять оказавшегося рядом человека. После того, как тот берет карту, злоумышленник проверяет ее баланс и утверждает, что с его счета пропали деньги и вынуждает вернуть доставшего карту человека эту сумму. В используемой злоумышленниками схеме могут участвовать двое или трое — еще один человек будет изображать «свидетеля» кражи денег с карты. Притворившийся пострадавшим злоумышленник начнет угрожать вызвать полицию, обосновывая это тем, что на его карте остались чужие отпечатки пальцев, и якобы будет легко доказать предполагаемую пропажу денег с карты.

На самом же деле никакой кражи денежных средств от прикосновения к карте не происходит, мошенники пытаются заполучить денежные средства путем запугивания и обмана оказавшегося рядом человека.

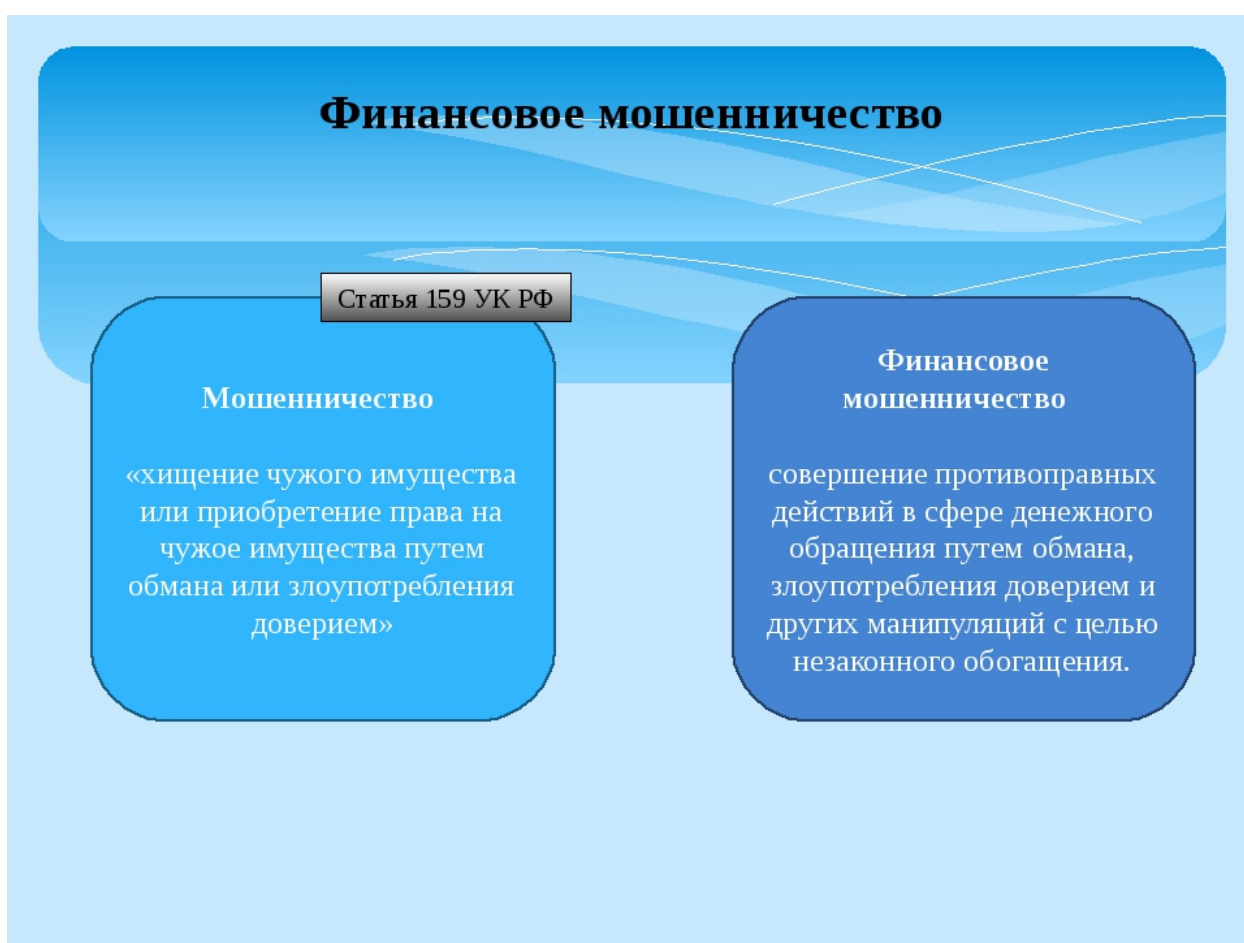
Компрометация ПИН-кода держателем банковской карты. Под этим понимается запись ПИН-кода непосредственно на карте или на каком-либо носителе (лист бумаги, записная книжка, мобильный телефон), хранимом вместе с картой. Если банковская карта утеряна или украдена (обычно вместе с бумажником, барсеткой, сумочкой), то у вора оказывается и карта, и персональный код. В таком случае мошенникам совсем нетрудно несанкционированно использовать банковскую карту для получения наличных денежных средств и/или оплаты товаров (услуг).

Дружественное мошенничество. Член семьи, близкий друг, коллега по работе, имея доступ к месту хранения банковской карты, берет ее без разрешения ее держателя, а затем, предварительно узнав ПИН-код,

Среди всех видов мошенничеств особое место занимает финансовое мошенничество. В наши дни мошенничество приобрело интеллектуальный характер.

В данной статье разберём, что такое финансовое мошенничество, какие виды существуют, как себя обезопасить и какая ответственность предусмотрена за мошенничество.

Снифферинг – это способ мошенничества, при котором злоумышленник использует анализатор проходящего трафика Интернет-сети («сниффер») – специальную компьютерную программу для перехвата данных с возможностью их декодирования и анализа. Снифферинг особенно популярен в людных местах, везде, где есть общедоступная сеть wi-fi.



Наиболее часто встречаются схемы финансового мошенничества на которых видны основные принципы.

Современные финансовые мошенничества многообразны:

1. Интернет-мошенничество.
2. Мошенничество с использованием банковских карт.

3. Финансовые пирамиды.

1. Интернет-мошенничество

- **Покупки через интернет.** Продавец просит оплатить товар через систему денежных переводов, используя фальшивое удостоверение личности. Когда он получает деньги то сразу исчезет.

- **Письма платежных систем,** к которым прилагается вирус, замаскированный под вложение-файл или ссылку. Его задача собрать данные об ваших аккаунтах в платежных системах и данные банковских карт.

2. Мошенничество с использованием банковских карт.

- **Скимминг**-это установка специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте: накладная клавиатура или маленькая камера которая заснимет ввод ПИН-кода, и устройство для считывания данных карты.

- **Траппинг**-на банкомат устанавливаются устройства которые блокируют карту. На помощь человеку приходит мошенник, который подглядывает пин-код, и после ухода человека достает карту из банкомата. Ввод ПИН-кода нужно закрывать рукой.

3. Финансовые пирамиды.

Финансовые пирамиды предлагают своим клиентам заработать на инвестициях, на фондовом рынке. Обещают получение прибыли в крупных размерах. Фактически же цель этих организаций — собрать максимально средств с клиентов. - Признаки финансовых пирамид: высокая доходность за счет непрозрачных сверхприбыльных проектов в другой стране., отсутствие лицензий, обещание вознаграждения за приведенных друзей. Лучше принимать взвешенные решения, не поддаваться эмоциям.

Как себя обезопасить

- При краже карты — позвонить в банк, заблокировать карту.
- При получении смс-сообщения о списании суммы с вашего счета, получения запроса на подтверждение операции, которую вы не производили — позвонить в банк и уточнить об операции.
- Никому не сообщать номер банковской карты, пин-код; не давать пароль к доступу своего счета через интернет.
- Не передавать банковскую карту третьим лицам.
- Перед использованием банкомата, всегда внимательно его осматривать.
- Закрывать клавиатуру при вводе пин-кода банковской карты.
- При открытии подозрительных писем, не переходите по ссылкам.
- Не устанавливать подозрительные программы.
- Установить антивирусные программы.
- Не открывайте подозрительные письма.
- Не раскрывать ваши персональные данные, звонящим с незнакомых номеров

**МВД РОССИИ ПРЕДУПРЕЖДАЕТ**
будьте бдительны! звоните 02 или 102

НЕ ОТКРЫВАЙТЕ ДВЕРЬ незнакомым людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиники, ЖКХ и т.д. Перезвоните и уточните, направляли ли к Вам этого специалиста!





НЕ ДОВЕРЯЙТЕ, если Вам звонят и сообщают, что Ваш родственник или знакомый попал в беду или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку, купить дорогие лекарства - в общем откупиться. **Это ОБМАН!**

СЛЕДИТЕ ЗА СОХРАННОСТЬЮ ЛИЧНЫХ ДОКУМЕНТОВ
Аферисты рассказывают, что Вам положены некие выплаты или льготы, а чтобы их получить, надо подписать ряд документов. А вместо этого подсовывают на подпись доверенность или дарственную на Вашу квартиру!





Незнакомец сообщает о выигрыше, блокировке банковской карты, о пересчете квартплаты, срочном обмене денег на дому или предлагает приобрести товары и таблетки по низким "льготным" ценам? **НЕ ВЕРЬТЕ - ЭТО МОШЕННИЧЕСТВО!**