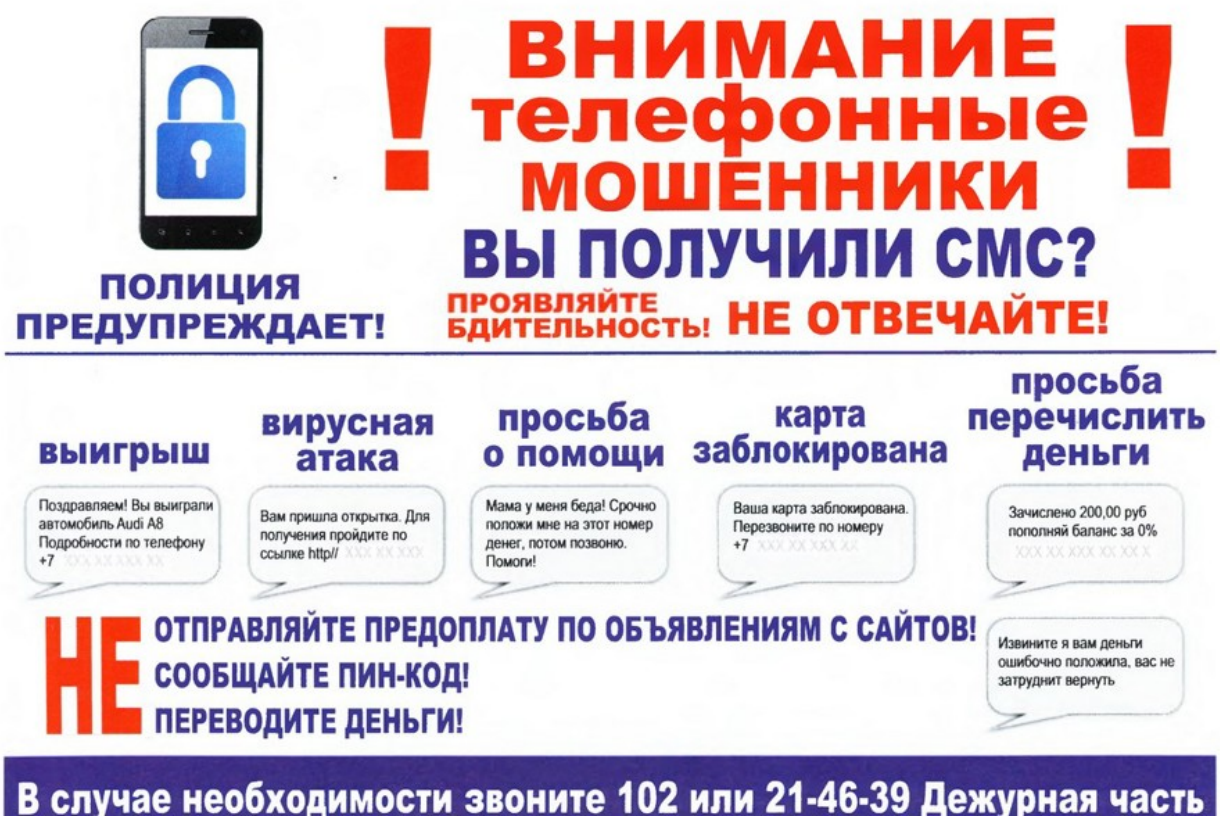
# Памятка по профилактике бесконтактных хищений

Опубликовано 01 декабря 2023
10:02




1. ***Способ хищения: Под видом банковского работника (сотрудника службы безопасности, сотрудника полиции, налоговой, прокуратуры и т.д.).***

Человеку поступает звонок, в ходе которого собеседник представляется сотрудником банка и сообщает, что кто-то пытается списать деньги, оплатить товары или услуги с банковской карты, или получить кредит на его имя на крупную сумму. И чтобы

сохранить сбережения, необходимо незамедлительно назвать ее реквизиты - это номер карты, трехзначный код на обратной стороне (CVV) и срок ее действия, или перечислить деньги на указанный «безопасный» счет.

***Примеры:***

1. Поступает звонок от сотрудника Центробанка России, который сообщает что он контролирует все банковские учреждения и в настоящее время от коллег поступила информация о том, что кто-то пытается оформить на его имя кредит на сумму 100 тыс. рублей. В ходе беседы преступник выясняет в каких банковских учреждениях у него имеются открытые счета. После чего предлагает отправиться в отделения банковских учреждений, при этом называет конкретные банки (*сбербанк, ВТБ, Алфа-Банк, МТС-банк, Газпромбанк*) и адреса их расположения и предлагает в указанных учреждениях оформить кредит, с целью перевода денежных средств на безопасный счет для их последующей сохранности.
2. Поступает звонок от сотрудника полиции, который сообщает что он расследует уголовное дело по фактам мошеннических действий, или поступили сведения об утечке информации из банковских учреждений, либо у него в разработке находится преступная группа, члены которой пытаются оформить на его имя кредит в банковском учреждении. Также он сообщает, что ему в настоящее время ему поступит телефонный звонок от лже сотрудника банка, которому он должен подыграть, в целях его изобличения.

Аферисты всегда торопят, чтобы у Вас не было времени все обдумать. Сильные эмоции притупляют бдительность.

***Признак хищения:*** попытка получить трехзначный код или перечислить деньги на «безопасный» счет, многочисленные звонки с разных номеров (IP-телефония)

***Способ защиты:*** ***Немедленно прекратить разговор – это мошенники!!!***

Не называть трехзначный код на обратной стороне (CVV), коды из СМС, PIN-код, пароли/логины к банковскому приложению и онлайн-банку, кодовое слово, персональные данные, и не перечислять деньги, позвонить на телефон банка, указанный на карте.

***Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС и не просят совершать переводы с Вашей карты.***

***Внимание! Банковская карта является ключом к счету. Поэтому никому ее не передавайте, не сообщайте ее реквизиты. В случае поступления информации о сомнительных операциях, обращайтесь непосредственно в банк или по телефону горячей линии, указанному на карте.***

2. ***Способ хищения:*** **Под предлогом получения кредита.**

Потерпевшему предлагают кредит на выгодных условиях.

***Признак хищения:*** для получения кредита предлагается предварительно оплатить комиссию, страховку, проценты по кредиту.

***Способы защиты:*** **Получать деньги в кредит в офисах кредитно-финансовых организаций.**

3. ***Способ хищения:*** **Звонки правоохранительных органов по расследованию преступлений в отношении банковских работников иных сотрудников.**

4. ***Способ хищения:*** **Звонки под видом вышестоящего руководства**

- в долг;

- для проверяющего, вышестоящего;

- иные сборы.

5. ***Способ хищения:*** **Под предлогом получения компенсации за ранее приобретенные товары, заманивают на распродажи.**

Преступник звонит гражданину и сообщает, что ему положена денежная компенсация, социальные выплаты или сверхприбыльные инвестиционные проекты.

***Признак хищения:*** необходимость предварительной оплаты за разные услуги для получения компенсации. **Гарантия быстрого обогащения – признак обмана. Огромные скидки и низкие цены могут оказаться мошеннической уловкой.**

***Способы защиты:*** не перечислять деньги незнакомцам, кем бы они не представлялись. Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения.

6. ***Способ хищения:*** **Под предлогом помощи родственникам, близким.**

Мошенники по телефону представляясь родственниками или их знакомыми, или сотрудниками правоохранительных органов по просьбе родственников, просят срочно перечислить, перевести деньги на банковский счет или по номеру телефона чтобы их «спасти от беды» (от уголовной и иной ответственности в результате ДТП, иного происшествия, или для экстренного лечения и т.д.)

***Признак хищения:*** срочность, ранее неизвестные номера телефонов.

***Способы защиты:*** **Перезвонить своему знакомому и уточнить что случилось.**

***Мошенники могут использовать различные уловки – представляться сотрудниками правоохранительных органов, вашими близкими, придумывать что угодно! Их главная цель – получить от вас деньги или реквизиты банковской карты! Помните об этом!***

7. ***Способ хищения:*** **Под предлогом займа денег.**

Мошенники получают доступ к взломанным аккаунтам в социальных сетях и под видом знакомых просят одолжить деньги.

***Признак хищения:*** знакомые просят взаймы через социальные сети.

***Способы защиты:*** **Перезвонить своему знакомому и уточнить о его просьбе.**

8. ***Способ хищения:*** **Связанные с СВО (Украина).**

- близкие родственники; - благотворительность; - перевод Украине;

9. ***Способ хищения:*** **с использованием поддельных телефонных номеров (IP телефония).**
10. ***Способ хищения:*** **При продаже товаров или оказании услуги (работ).**

Мошенник размещает в Интернете объявление о продаже товара (оказании услуги, работы) и просит перечислить деньги за товар.

**- в т.ч. интимные услуги и т.д.**

***Признак хищения:*** продавец просит предоплату за товар (за услугу).

***Способ защиты:*** **Не переводить деньги заранее. Потребовать у продавца отправить товар по почте с использованием услуги - описью вложения, а  опалить за услугу после ее предоставления.**

***Ни в коем случае нельзя совершать покупки в Интернете с использованием кредитной или зарплатной карты, где у вас могут быть крупные суммы денег!***

***Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой!***

11. ***Способ хищения:*** **Под предлогом покупки товара.**

Мошенник звонит под видом покупателя и просит назвать реквизиты банковской карты, в том числе трехзначный код, для оплаты.

***Признак хищения:*** Получение трехзначного кода.

***Способы защиты:*** Не называть секретный код, расположенный на обратной стороне карты и пароли, приходящие в смс-сообщениях!

12. ***Способ хищения:*** **С помощью вирусной ссылки.**

Приходит сообщение в виде ссылки, пройдя по которой обещают приз, интересное фото и т.д.

***Признак хищения:*** получение сообщения со ссылкой с неизвестного номера.

***Способы защиты:***

**Установите антивирус** и регулярно обновляйте его.

**Сохраняйте** в закладках адреса нужных сайтов.

**Не переходите** по подозрительным ссылкам.

***Вирусы открывают удаленный доступ к Вашему устройству, крадут логины  и пороли от онлайн-мобильного банка, перехватывают секретные коды из сообщений.***

***Заполучив эти данные, киберпреступники могут похитить все деньгт с Ваших счетов без Вашего непосредственного участия!***

-

13. ***Способ хищения:*** **С помощью сайта-подделки (фишинг).**

Создается копия известного сайта с указанием реквизитов для перечисления денег на счета мошенников.

***Признак хищения:*** сайт создан недавно, в названии имеет «http» вместо безопасного «https».

***Способы защиты:*** Убедится, что сайт настоящий, в названии сайта «https», а не «http». Проверить дату создания сайта - он должен быть создан достаточно давно.

14. ***Способ хищения:*** **найденные вещи, банковские карты, использование без спроса.**
15. ***Способ хищения:*** **Контактные мошенничества (*вовлечение в курьерство, в т.ч. по линии незаконного оборота наркотиков*).**

**Что делать, если с карты украли деньги?**

1. **Заблокировать карту** (*по номеру телефона банка на банковской карте или на официальном сайте; через мобильное приложение; лично в отделении банка*).
2. **Написать заявление в банк о несогласии с операцией (***заявление должно быть написано в течение суток после сообщения о списании денег на месте в отделении банка*).
3. **Обратиться в полицию.**

**МВД по Чувашской Республике**