Памятка
по профилактике бесконтактных хищений

1. ***Способ хищения:*** **Под видом банковского работника (*сотрудника службы безопасности, полиции, 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 оформить 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.

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 и не перечислять деньги, позвонить на телефон банка, указанный на карте.

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:*** **При продаже товаров или оказании услуги (работ) (*с использованием сайтов «Авито», «Юла», «AliExpress» и т.д.*).** Мошенник размещает в Интернете объявление о продаже товара, оказании различных услуг, работы (*под предлогом трудоустройства, аренды жилья, оказания интим услуг, оказания услуг по перевозке через приложение «BlaBlaCar» и т.д.*) и просит перечислить деньги за товар или за оказанные услуги.

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!

3. ***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!**

4. ***Способ хищения:*** **Торговля на валютных биржах, участие в коммерческих организациях и фондах.** Мошенники предлагают различные финансовые инвестиции (*покупка акций, ценных бумаг, биткоинов, криптовалюты*) на выгодных условиях, с целью получения значительной прибыли.

***Признак хищения*:** необходимость открытия брокерского счета, обязательная регистрация, установка демонстративной программы, щедрость предложений, для вывода денежных средств необходимо подключить разовый страховой полис, невозможность выведения вложенных денежных средств.
Способы защиты: **не перечислять деньги незнакомым лицам, кем бы они не представлялись.**

4. ***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!

5. ***Способ хищения:*** **Под предлогом займа денег** ***(через приложения «WhatsApp», «Viber», «ВКонтакте», «Одноклассники»***). 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.**

6. ***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.**

7. ***Способ хищения:*** **Под предлогом получения различных выигрышей, бонусов, компенсации за ранее приобретенные товары (*биологические активные добавки*).** Преступник звонит гражданину и сообщает, что ему положена денежная компенсация.
Признак хищения: необходимость предварительной оплаты за разные услуги для получения компенсации.
Способы защиты: **не перечислять деньги незнакомцам, кем бы они не представлялись.**

8. ***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: **Не открывать ссылки с неизвестных номеров. Установить на телефон антивирусную программу.**

9. *Способ хищения:* С помощью сайта-подделки (*«фишинговый» сайт*). 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: **Убедиться, что сайт настоящий, в названии сайта «https», а не «http». Проверить дату создания сайта - он должен быть создан достаточно давно.**

10. *Способ хищения:* Звонки от вышестоящих руководителей. Мошенники от имени вышестоящих руководителей просят передать, перечислить денежные средства, оказать различные услуги.
Признак хищения: срочность, ранее неизвестные номера телефонов.
Способы защиты: **Перезвонить своему руководителю и уточнить о его просьбе.**

11. *Способ хищения:* Поступают звонки с номеров государственных органов. Человеку поступает звонок, в ходе которого собеседник представляется сотрудником государственных органов и сообщает, что кто-то пытается списать деньги, оплатить товары или услуги с банковской карты, или оформить кредит на его имя на крупную сумму.
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 и не перечислять деньги, позвонить на телефон банка, указанный на карте.

12. *Способ хищения:* Утеря сотовых аппаратов, банковских карт, паспорта гражданина Российской Федерации.
***Способы* защиты: Принять меры по незамедлительной блокировке банковских карт, обратиться в органы внутренних дел с заявлением об утере паспорта гражданина Российской Федерации.**

В любых случаях мошенничества необходимо НЕЗАМЕДЛИТЕЛЬНО позвонить в дежурную часть МВД по Чувашской Республике по телефону 020.