Приложение

Памятка

по профилактике бесконтактных хищений

1. ***Способ хищения:*** **Под видом банковского работника**. Человеку поступает звонок, в ходе которого собеседник представляется сотрудником банка и сообщает, что кто-то пытается оплатить товары или услуги с банковской карты, 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.

Способ защиты: **Не называть трехзначный код и не перечислять деньги, позвонить на телефон банка, указанный на карте.**

2. ***Способ хищения:*** **При продаже товаров**. Мошенник размещает в Интернете объявление о продаже товара и просит перечислить деньги за товар.

Признак хищения: продавец просит предоплату за товар.

Способ защиты: **Не переводить деньги заранее. Потребовать у продавца отправить товар по почте с использованием услуги – описью вложения.**

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:*** **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.**

5. ***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.**

6. ***Способ хищения:*** **Под предлогом получения компенсации за ранее приобретенные товары.** 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.**

7. ***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.**

8. ***Способ хищения:*** **С помощью сайта-подделки.** 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.**

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

Для избежания потери крупной суммы денег, необходимо завести дополнительную дебетовую банковскую карту с отдельным счетом, и

пополнять ее на ту сумму, которая необходима. И ни в коем случае нельзя совершать покупки в Интернете с использованием кредитной или зарплатной карты, где могут быть крупные суммы денег!

Мошенники могут использовать различные уловки – представляться сотрудниками правоохранительных органов, родственниками, друзьями, придумывать что угодно! Их главная цель – получить деньги или реквизиты банковской карты! Помните об этом!