Приложение № 1

Памятка

по проведению беседы с гражданами о возможных формах и методах совершения хищений чужого имущества бесконтактным способом, а также способах противодействия таким преступлениям

В настоящее время распространены следующие виды хищений бесконтактным способом: кражи с банковских карт, факты мошенничества и вымогательства.

Бесконтактная кража с банковских карт – это хищение денежных средств граждан, при котором под любыми предлогами и видами преступник завладевает реквизитами банковской карты, с помощью которых впоследствии совершает перевод или снятие денег.

Отличие бесконтактной кражи от бесконтактного мошенничества в том, что при совершении кражи, потерпевший не переводит деньги злоумышленнику, а лишь сообщает данные о своей карте преступнику, или теряет ее, а преступник производит перевод или снятие денежных средств. При **мошенничестве потерпевший сам переводит деньги лицу**, которое получив их, впоследствии, не оказывает обещанные услуги и не возвращает деньги.

Вымогательство, совершаемое бесконтактным способом – это такой способ отъема у граждан денег, при котором злоумышленник зачастую требует передачи ему денежных средств в обмен на нераспространение в социальных сетях, мессенджерах и т.п. информации о потерпевшем (фото, видео) дискредитирующего характера, чаще всего интимного свойства.

Преступления совершаются дистанционно, без непосредственного контакта с потерпевшим, под различными видами и предлогами. Наиболее распространены следующие:

1. Под видом покупки (продажи) различных товаров на Интернет-сайтах объявлений. Злоумышленник предлагает начать общение в иных мессенджерах таких, как «Ватсап», где пересылает Интернет-ссылку, по которой нужно пройти и ввести реквизиты своей банковской карты для

зачисления денежных средств, вместо этого происходит их списание (хищение). Затем ссылка становится нерабочей.

Направление сообщений с Интернет-ссылками для перехода и оплаты товара от имени проверенных Интернет-магазинов также возможно и в ином мессендежере таком, как «Вайбер».

2. Под видом банковских работников, под следующими предлогами:

- разблокировка счета якобы заблокированной карты;

- приостановление несанкционированного снятия денежных средств с карты;

- предоставление кредита;

- страхование счетов и вкладов.

НЕОБХОДИМО ЗАПОМНИТЬ: СОТРУДНИКИ БАНКА НИКОГДА НЕ СПРАШИВАЮТ РЕКВИЗИТЫ КАРТ (НОМЕР, ТРЕХЗНАЧНЫЙ КОД С ОБОРОТНОЙ СТОРОНЫ, смс-коды, которые приходят на сотовый телефон).

Если после слов якобы сотрудника банка закрались сомнения, необходимо обратиться в любое отделение банка, либо позвонить на номер, указанный на обратной стороне Вашей карты.

3. **Посредством социальных сетей, путем взлома «аккаунтов»** потерпевших, под предлогом займа денег *(чтобы себя перестраховать необходимо перезвонить лицу, которое просит у Вас деньги. Если нет телефона - спросить у него информацию, которую можете знать только вы и он (она)).*

4. Под предлогом оказания различных услуг (аренда жилья, снятие порчи, изготовление научных работ, интим, уход за больными и пожилыми).

5. Под предлогом выплаты денежной компенсации за ранее приобретенные БАДы, лекарства и пр. *Представиться могут кем угодно, но как только разговор заходит, что Вам надо заплатить деньги, чтобы получить компенсацию или комиссию, налог или еще какую-нибудь материальную выгоду, необходимо немедленно завершить разговор. Это уловка, чтобы выманить у Вас деньги.*

6. При покупке товаров через Интернет наложенным платежом в почтовом отделении (получает не то, что заказывал. Как пример, опилки вместо штор). ЧТОБЫ БЫЛА ВОЗМОЖНОСТЬ ВОЗМЕЩЕНИЯ УЩЕРБА,

необходимо чтобы посылка была с описью вложения (оформляется отправителем).

Но существуют и способы защиты:

1. Никому и никогда нельзя сообщать реквизиты банковской карты (номер карты, трехзначный код, а также смс-коды, которые приходят на номер мобильного телефона, к которому привязана карта).

Запомните, сотрудники банков никогда не спрашивают эту информацию. Она является конфиденциальной.

2. Для владельцев кредитных карт с бесконтактным способом оплаты рекомендуется установить минимальный кредитный лимит при оплате без пин-кода или вовсе его отменить.

3. Не отдавать банковскую карту третьим лицам ни под каким предлогом, а тем более сообщать пин-код, ведь это секретная информация, которая доступна только владельцу карты, даже сотруднику банка она неизвестна.

4. Не стоит производить оплату в ответ на смс-сообщения и электронные письма, пришедшие от неизвестных источников.

5. Не переходить по Интернет-ссылкам, направленным в мессенджерах лицами, выступающими в качестве покупателей на бесплатных сайтах объявлений «Авито», «Юла», либо в качестве водителей - при заказе поездки посредством приложение «Бла-бла-кар».

5. Не стоит устанавливать на свои устройства по просьбе иных лиц программное обеспечение.

6. Также не нужно верить, что вам звонят сотрудники банка. Получив подозрительный звонок, лучше сразу положить трубку, найти актуальный номер «горячей линии» вашей кредитной организации, а затем самостоятельно позвонить и уточнить, все ли в порядке с картой. ПЕРЕЗВАНИВАТЬ НА ПОДОЗРИТЕЛЬНЫЙ НОМЕР НИ В КОЕМ СЛУЧАЕ НЕ СЛЕДУЕТ.

Преступники привыкли играть на психологии человека – они либо пугают жертву возможной потерей средств, либо лгут о неком случайном денежном выигрыше, который можно получить, лишь сообщив конфиденциальную информацию. Таким образом, создается стрессовая

ситуация, подталкивающая человека к поспешным и необдуманным действиям.

Если же с Вашей карты деньги похищены без Вашего ведома, необходимо позвонить в банковское учреждение по номеру, указанному на обратной стороне карты. Следует сообщить об исчезновении денежных средств с карточного счета и следовать всем предписаниям банка. Если Вы уверены, что не совершали никаких операций по карте (и родственники, и близкие не причастны), нужно обратиться в банк с заявлением о возврате денег. Если банк отказывает, можно обратиться в суд. Вернуть исчезнувшие средства крайне сложно, особенно если для проведения транзакций необходим ввод пин-кода, но можно попытаться.

МВД по Чувашской Республике