Основные виды дистанционных мошенничеств

1) Звонок службы безопасности банка:

Принцип действия: на телефон человека звонит неизвестный и, представившись сотрудником службы безопасности банка, сообщает о том, что по счету его банковской карты происходят подозрительные операции либо осуществлена попытка платежа или перевода. После этого узнают у потерпевшего реквизиты банковской карты (номер, код безопасности, срок действия карты) и коды, пришедшие в СМС-уведомлениях. В результате указанных действий осуществляют перевод денежных средств на другие счета путем подключения к онлайн-банку потерпевшего.

Также мошенники путем обмана уговаривают граждан внести денежные средства через терминал на счета банковских карт либо абонентских номеров на так называемый «резервный счет».

По такой же схеме предлагают взять кредит, внести денежные средства через терминал на указанный мошенниками счет.

2) Звонок представителя органа власти или правоохранительного органа:

Принцип действия: на телефон человека звонит неизвестный и представляется сотрудником какого-либо органа власти или правоохранительного органа. ФИО и должность сотрудника могут быть как вымышленными, так и настоящими, которые размещены на сайте указанных органов. Мошенник сообщает, что в отношении гражданина возбуждено уголовное дело и предлагает его «закрыть», предлагает повышение по службе, оказание каких-либо муниципальных или государственных услуг. За все эти действия мошенник просит осуществить перевод денежных средств.

3) Покупка/продажа товара через сайт «Авито»:

Принцип действия: злоумышленник размещает объявление на известных досках объявлений – АВИТО, ЮЛА, JOOM, ВКОНТАКТЕ, INSTAGRAM о продаже товара по заниженной стоимости (ниже рыночной), с подробным описанием состояния и условий использования. Общение с потерпевшим

осуществляет в ходе переписки в интернет-мессенджерах, в редких случаях путем телефонного разговора. Предлагает внести предоплату за товар, отправляет реквизиты банковской карты, после получения денежных средств мошенник, как правило, не выходит на связь.

Пример: *Гражданка разместила на сайте «Авито» объявление о продаже обуви – босоножек за 1500 рублей, где указала свой номер телефона. Через мобильное приложение «WhatsApp» написала «неизвестная» и поинтересовалась приобретением босоножек. В ходе общения женщина указала, что находится в г. Вельске, попросила отправить товар через транспортную компанию СДЭК, и скинула ссылку для оплаты доставки. Перейдя по ссылке там было указано — вкладка «Получить денежные средства», и в специальном окне продавец ввела все реквизиты банковской карты и код безопасности с обратной стороны карты, а также ввела код из поступившего смс-сообщения-уведомления. Далее с банковской карты произошло списание денежных средств.*

4) Оказание услуг такси «Бла-Бла-Кар»:

Принцип действия: мошенники размещают на «BlaBlaCar» объявления о свободных местах в машине, ничем не отличающиеся от настоящих. Когда пользователь откликается на объявление, мошенники в чате на сайте «BlaBlaCar» просят его связаться с ними в мессенджере «WhatsApp» и отправляют номер телефона. Мошенники требуют предоплату через сайт. После ввода данных карточки на мошенническом сайте, у жертвы мошенников со счета исчезают все деньги.

Чтобы не стать жертвой мошенников следуйте следующим правилам:

1. Ни в коем случае не сообщайте свои персональные данные, номера банковских карт, пин-коды от них и не выполняйте денежных операций.
2. Помните, сотрудники службы безопасности банка, органа власти или правоохранительного органа сами никогда не звонят!

3. Если Вам звонит лицо, представившись сотрудником органа власти или правоохранительного органа, не переводите денежные средства, уточняйте информацию по телефонам, указанным на официальных сайтах органов.

4. Не осуществляйте покупки у непроверенных продавцов, не вносите предоплату, не переходите по ссылкам, в которых необходимо ввести данные своей карты, не осуществляйте оплату за товар, не проверив его.

5. Не переходите по посторонним ссылкам, которые скидывают злоумышленники, не вводите реквизиты Ваших карт в сети «Интернет».