Информация для населения о схемах и способах, используемых при совершении преступлений с применением современных средств коммуникации и связи.



В настоящее время, наблюдается стремительный рост преступлений, совершенных с использованием современных средств связи и коммуникации.

Преступники, умело пользуясь доверчивостью граждан, стараются заполучить данные клиентов банков самыми различными способами, как правило, через прямой контакт с потенциальным потерпевшим.

Если человек сообщает мошенникам свои данные для проведения операций (номера карт, логины и пароли для входа в личный онлайн-кабинет, одноразовые СМС-пароли), то у злоумышленников появляется полный доступ к банковскому счету.

Ярким и частым примером являются случаи, когда к вам на телефон поступает либо СМС сообщение, либо звонок от сотрудника службы безопасности банка о том, что ваш счет заблокирован и Вам необходимо сообщить данные карты. После того, как гражданин сообщает эти сведения, преступники получают доступ к счету и переводят с него денежные средства.

В ряде случаев, под видом сотрудников служб безопасности банков, либо даже представляясь сотрудниками правоохранительных органов, мошенники просят своих жертв перевести деньги на «резервный счет» для их сохранности.

Конечно же, никакого резервного счета у банка нет и быть не может, мошенники пользуются доверчивостью граждан, которые в итоге сами переводят деньги на их счета. Яркий пример, когда вам звонит мошенник, представившись сотрудникам банка и говорит, что ваш счет пытались взломать и необходимо перевести деньги на

другой счет, то есть резервный. Данный вид преступления совершается при активном использовании подмены номера, что позволяет мошенникам имитировать звонки, к примеру, из Москвы, хотя сам человек при этом находится в другом городе. Это дает злоумышленникам возможность успешно маскироваться под сотрудников банковских организаций. Во избежание таких случаев, даже если поступает звонок с номера телефона, похожего на номер банка, но при этом «сотрудник» просит сообщить конфиденциальную информацию, необходимо просто положить трубку и перезвонить в банк по номеру телефона, указанному на сайте банка или оборотной стороне банковской карты. В зоне риска оказываются граждане, которые что-то продают или покупают на сайтах бесплатных объявлений или в социальных сетях, а также те, с кем мошенники вступают в переписку со странички «взломанного» друга.

Ни в коем случае нельзя соглашаться на перевод денежных средств за понравившуюся вещь на мобильный телефон продавца, так как в большинстве случаев это элемент преступной схемы.

Также не стоит обращаться по объявлениям о товаре, цена на который явно занижена.

Еще одним высокотехнологичным способом хищения является вирусное заражение компьютеров и мобильных телефонов. Наиболее подвержены вирусной атаке клиенты банков, использующие СМС-банкинг и мобильные банковские приложения на таких устройствах.

Вирусы могут распространяться как через СМС, ММС-сообщения, так и через популярные мессенджеры, что резко снижает возможность их выявления со стороны операторов сотовой связи.

Преступления данного вида совершаются следующим образом, владелец смартфона получает сообщение, в тексте которого имеется ссылка, при открытии инициирующая загрузку вирусной программы. Как только вирус попадает в смартфон, он начинает рассылать СМС по контактным листам пользователя. Параллельно он делает запрос на номер СМС-банка и узнает баланс счета владельца смартфона. После этого вирусная программа переводит деньги на счета, подконтрольные злоумышленникам. Вирус способен перехватывать входящие СМС-сообщения, поэтому владелец смартфона может не знать о снятии денег со счета, ведь оповещения о списаниях не доходят. Кроме того, вирус может открывать окна браузера, визуально похожие на окна авторизации банковских приложений, и при

вводе данных своих карт пользователи отправляют средства напрямую мошенникам. В некоторых случаях вирус может блокировать смартфон.

С целью защиты электронных устройств от вирусных атак, необходимо обеспечивать их антивирусной защитой.

Таким образом, если раньше преступникам требовалось получить физический доступ к деньгам жертвы, то теперь достаточно получить доступ к конфиденциальной информации. Именно при помощи такой информации, которую граждане зачастую сами охотно сообщают аферистам, последним удается удаленным способом похитить любые суммы денежных средств, вывести их на любые выбранные ими счета и обналичить в любой точке мира. Реагировать на подобные звонки и сообщения следует спокойно и рассудительно, не поддаваться на уговоры, обязательно проверить информацию. Если вам сообщили о блокировке карты, необходимо обратиться в ближайшее отделение банка, либо по телефону, указанному на банковской карте.

Если вам сообщили о том, что кто-то из родственников попал в неприятности, необходимо задать контрольный вопрос, ответ на который знаете только вы и родственник, а лучше всего дозвониться до последнего, либо до других родственников.

Ни в коем случае нельзя сообщать по телефону информацию, касающуюся банковской карты, персональных данных и наличие на ней денежных средств.

При дистанционном общении важно учитывать, что если с вас требуют предоплату для выполнения условий договора купли-продажи, устройства на работу, получения выигрыша, в отношении вас совершаются противоправные действия.

При смене СИМ-карты не забывайте отключать мобильный банк. Если вы заподозрили, что перевели деньги злоумышленникам, то следует немедленно отменять операцию.

Важно понимать, что сохранность ваших сбережений в большей степени зависит от вас, будьте бдительны, проверяйте информацию любым доступным для вас способом.

Поэтому, если вам позвонили или прислали СМС подозрительного содержания, либо вы наткнулись на мошенническое объявление, обязательно сообщите об этом в полицию.