Профилактика хищений, совершаемых дистанционно

Одним из самых динамично развивающихся направлений преступных посягательств в настоящее время являются хищения денежных средств, которые совершаются с использованием информационно-телекоммуникационных технологий (it-технологий) с помощью современных средств связи, компьютерных программ, Интернета и пр.

Основное отличие этих преступлений в том, что личного контакта потерпевшего и преступника не происходит. Общение происходит по телефону, в социальных сетях, в различных мессенджерах (вайбер, ватсап, телеграмм). Преступника и жертву могут разделять тысячи километров.

В первом полугодии 2020 года на территории Кировской области возбуждено более 2 000 уголовных дел по кражам и мошенничествам, которые были совершены дистанционно. Общий ущерб составил более 100 млн рублей.

В Тужинском районе совершено 9 преступлений, потерпевшие лишились около 500000 рублей.

Раскрываются такие преступления сложно (раскрываемость по Кировской области составляет около 15%). Полиция обращает внимание граждан, что преступления всегда легче предупредить, зная те действия, которые помогут уберечь свои сбережения от хищений.

Наиболее массовыми в последнее время стали факты дистанционного хищения с банковских карт и счетов граждан. Преступники используют предоставленные самими гражданам возможности управлять своими денежными средствами через мобильный телефон или компьютер — переводить деньги, оформлять

кредиты, совершать покупки в Интернет-магазинах и др. Преступники имеют умения и навыки по работе с различными банковскими сервисами, их познания о различных способах денежных переводов выше, чем у обычного гражданина.

Цель мошенника – получение путем обмана конфиденциальной информации о банковской карте потерпевшего, либо скрытое управление потерпевшим, в результате чего он сам переводит деньги на счета преступников.

Основные способы.

1. Преступники звонят гражданам, которые разместили объявления о продаже каких-либо товаров или предоставлении услуг на сайтах бесплатных объявлений, чаще всего на сайте «Авито». Предлагают внести предоплату и просят назвать реквизиты банковской карты: ее номер, срок действия, CVC-код на обратной стороне карты, а также цифровые пароли, поступающие на мобильный телефон — puch-код. С помощью информации, которую передает преступнику сам гражданин, совершается хищение.

2. Мошенники рассылают СМС-сообщения , либо совершают обзвон, и сообщают абонентам ложную информацию о якобы возникших проблемах с банковской картой. В последнее время особенно часто мошенники называются сотрудниками службы безопасности банка. Потенциальную жертву подкупает то, что номер телефона звонящего зачастую похож на настоящий номер банка. Практически всегда собеседник обращается к потерпевшему по имени и отчеству. В результате гражданин выполняет инструкции злоумышленника по переводу средств на, так называемые, «безопасные счета», телефонные номера в результате чего лишается своих денег.

Все владельцы банковских карт должны знать, что сотрудники банков никогда не звонят своим клиентам для того, чтобы узнать информацию по счету, попросить сделать какие-то переводы. Работники кредитных организаций обладают всей необходимой информацией и инструментами для обеспечения безопасности находящихся на счетах денежных средств без привлечения клиентов. Для выяснения любой сомнительной ситуации необходимо гражданам самим звонить в банк по телефону, указанному на карточке.

Современные компьютерные программы (it-технологии) позволяют преступникам использовать, так называемые, «подменные номера». Гражданину поступает звонок на телефон, который определяется как номер дежурной части полиции, диспетчерской службы, номер горячей линии банка или другой знакомый ему номер. Потерпевший вводится тем самым в заблуждение и выполняет требования мнимых сотрудников правоохранительных органов, служб безопасности.

В таких случаях не надо вести переговоры, положите трубку и перезвоните сами по данному номеру. Так вы исключите общение с мошенниками.

3. Получили распространение факты хищения с банковских счетов без волевого участия потерпевшего. Когда ни СМС-сообщений, ни телефонных звонков клиенту банка не поступало, при этом операция по переводу денежных средств осуществлялась без его ведома. Во всех таких случаях потерпевшие являлись пользователями услуги «мобильный банк» и устройств сотовой связи. При переходе по ссылке на какой-либо Интернет-ресурс на смартфон потерпевшего устанавливалось приложение, которое дает возможность неизвестным лицам осуществлять банковские операции без его ведома. При этом

блокируется поступление от кредитной организации СМС-сообщений с информацией о проводимых операциях.

Рекомендации по безопасности:

1. Не передавайте незнакомцам реквизиты ваших банковских карт. Не сообщайте коды и пароли подтверждения банковских операций из СМС сообщений.
2. Не переводите денежные средства незнакомым лицам на неизвестные вам счета. При возникновении любой проблемы с счетом обращайтесь в отделение банка.
3. Применяйте уникальные пароли для своих учетных записей.
4. Не пренебрегайте использованием двухфакторной аутентификацией при использовании он-лайн сервисов.
5. Контролируйте разрешения в мобильных приложениях.
6. Остерегайтесь поддельных сайтов (проверяйте адрес сайта, чтобы не попасть на сайт-клон, который отличается от настоящего всего на одну букву, знак).
7. Не размещайте на общее обозрение, в том числе в социальных сетях, свои персональные данные (паспортные данные, реквизиты банковских карт).
8. Не спешите переводить деньги знакомым и родственникам на их просьбы в социальных сетях. Их аккаунты могут быть взломаны преступниками и использоваться для введения вас в заблуждение. Перезвоните по телефону и уточните, действительно ли, вашим близким требуется помощь.
9. Пользуйтесь услугами наложенного платежа при приобретении товаров, к посылке должна быть приложена опись.