

ОСТОРОЖНО-МОШЕННИКИ!!!!!!

Основной обновленной мошеннической схемой на сегодняшний день, где чаще попадают граждане пожилого возраста, это когда держателю банковской карты приходит SMS-сообщение, либо осуществляется звонок, (в основной массе номер телефона злоумышленника начинается с цифр 8-495...) и **МОШЕННИК, ПОД ПРЕДЛОГОМ ЗАЩИТЫ БАНКОВСКОЙ КАРТЫ ОТ НЕСАНКЦИОНИРОВАННОГО СПИСАНИЯ ДЕНЕЖНЫХ СРЕДСТВ**, начинает выманивать у потерпевшего реквизиты его банковской карты PIN-код и CVC2/CVV2 (код безопасности - цифры с обратной стороны карты), а также срок её действия и свои персональные данные, т.е. аналогично предлогу разблокировки банковской карты.

Следует знать и помнить, что ни один работник банка никогда не будет интересоваться реквизитами Вашей банковской карты, при отмене операции, как минимум при звонке, осуществленном из банка, работник
В ПЕРВУЮ ОЧЕРЕДЬ ПОИНТЕРЕСУЕТСЯ, ВЫ ЛИ ОСУЩЕСТВЛЯЛИ ОПЕРАЦИЮ!!!! А если даже у Вас действительно появилось сомнение, то необходимо связаться с банком, осуществить звонок на горячую линию, номера телефонов всегда оставляет любой работник банка, поинтересоваться проходили ли какие-то операции или попытки перевода денежных средств с Вашего счета, ну или как минимум попросить человека который с Вами связался и представился работником банка, любые Ваши данные, хотя бы фамилию.

Второй схемой, где также попадают граждане пожилого возраста, это когда держателю банковской карты **приходит SMS-сообщение о блокировании его банковской карты**, и также указан номер телефона «службы технической поддержки», как правило, начинающийся на 8-800-... Когда он перезванивает по указанному номеру, ему отвечает якобы сотрудник техподдержки банка и просит его подойти к банкомату и диктует ему ряд действий, чтобы снять блокировку карты. Далее, владелец «заблокированной» карты вводит и сообщает известные только ему данные, после чего с карты списываются имеющиеся денежные средства. Несмотря на то, что граждан при получении банковской карты предупреждают, чтобы они не сообщали никакой информации о своей карте: PIN-код и CVC2/CVV2 (код безопасности - цифры с обратной стороны карты), а также срок её действия и свои персональные данные посторонним лицам. При вхождении в приложение Сбербанк-Онлайн в SMS-уведомлении также дублируется информация о том, чтобы никому из посторонних не сообщали присланный код. **Сотрудники банков никогда не запрашивает эту информацию, такие случаи носят мошеннический характер.** В случаях сомнительных действий необходимо позвонить по телефонам указанным на банковской карте и заблокировать карту для прояснения ситуации.

Старая «классическая» схема мошенничества, на которую продолжают попадать лица пожилого возраста: **мошенники звонят преимущественно в**

ночное и вечернее время и сообщают, что «мам (бабуль) я попал в ДТП или в полицию» и просят денег для «решения вопроса». Далее в разговор вступает другой мошенник, который представляется сотрудником полиции и уверенно сообщает, что уже не раз помогал людям таким образом. Деньги, необходимо привезти в определенное место и передать конкретному человеку либо за ними приедет их знакомый человек, либо перевести на указанный счет.

Еще одним распространенным видом мошенничества являются мошеннические действия при купле-продаже товара по объявлению, размещенному на одном из многочисленных интернет-сайтов. При этом злоумышленник, может, как продавать, так и покупать товар.

При продаже товара злоумышленник, как правило, просит предоплату, сопровождая свою просьбу различными предложениями: срочно нужны деньги, уже нашелся другой покупатель и т.п. После перевода денежных средств в качестве предоплаты, как правило, связь с продавцом прекращается.

При покупке, злоумышленник приобретает товар, не торгуясь, либо вносит предоплату за съем жилья (квартиры, дома), имитируя спешку, невнимательность. Он якобы (один из вариантов мошенничества) переводит сумму больше, чем просит продавец, но на самом деле проходит регистрацию в приложении Сбербанк-Онлайн, при этом убеждает продавцов сообщать ему все присланные логины и пароли, а затем осуществляет переводы денежных средств с различных счетов продавца на счет его же банковской карты и просит часть денег перевести обратно.

Все виды мошенничеств и краж денежных средств с банковских карт, совершаемых дистанционным способом, невозможно описать, т.к. они постоянно видоизменяются, но способы защиты от них остаются неизменными:

Не сообщайте никому PIN-код и CVC2/CVV2 (код безопасности - цифры с обратной стороны карты), а также срок её действия и свои персональные данные. Ни один банк не будет по телефону спрашивать у вас эти реквизиты. Для зачисления средств на ваш счёт достаточно лишь 16значного номера, указанного на лицевой стороне карты.

Не сообщайте неизвестным лицам PIN-код для входа в ваш онлайн-банк - для перевода денежных средств это не требуется.

Не используйте карты с основным своим финансовым капиталом для оплаты в сети Интернет.

Не рекомендуется входить в интернет-банк с чужих компьютеров или из публичных незащищенных сетей Wi-Fi.

На личном компьютере, смартфоне, планшете установите антивирусное программное обеспечение и своевременно его обновляйте.

Не скачивайте файлы из непроверенных источников (файлообменные сервисы, социальные сети). Не переходите по ссылкам на информационные ресурсы, полученных от сомнительных источников. Не открывайте файлы из подозрительной электронной почты.

При звонке о попавших родственниках в полицию: не паникуйте, задайте вопросы личного характера (хотя бы как зовут ваших родственников и их близких), прервите разговор и попытайтесь связаться с тем родственником, который якобы попал в беду;

При просьбе об одолжении денег в долг, поступившей в социальных сетях, убедитесь, что просьба пришла именно от того лица, которое просит - просто перезвоните ему.

Также на сегодняшний день продолжают иметь место и так называемые социальные преступления, мошенничества и кражи совершаемые в отношении престарелых граждан.

При совершении социальных преступлений, преступники представляясь работниками различных социальных служб, горгаза, водоканала, беженцами Донбасса, под предлогом снятия порчи, попадают в жилище граждан. Как правило жертву высматривают в районе поликлиник, продуктовых магазинов, рынков, все это происходит в дневное время, примерно с 10 утра до 15-16 часов, входя в доверие к гражданам проникают в жилище, где совершают хищение денежных средств и других товарноматериальных ценностей.

У всех граждан нашей области имеются пожилые родственники, которые в силу возраста и незнания могут стать жертвами мошенников:

- Необходимо с ними постоянно проводить беседы, т.к. зачастую одного разговора не достаточно, чтобы уберечь их от действия злоумышленников.

Разъяснять, что денежные средства со счета даже сберегательной книжки можно перевести на счет банковской карты не посещая отделения банка, это может сделать любой человек, даже без наличия банковской карты.

Также необходимо разъяснять, что входную дверь необходимо всегда держать закрытой, не открывать, не убедившись в том, что человек представляющийся сотрудником газовой службы (или социальным работником, медицинским, из пенсионного фонда, из водоканала и др.) является действительно сотрудником этой службы - позвоните в указанную службу, уточните действительно ли осуществляется обход (обмен, проверка и т.п.).

При любом сомнении пожилых людей в действиях посторонних лиц, просите их, чтобы звонили Вам!!!

Начальник ОУУПиПДН

МОТд МВД России «Велижское»

В.А. Крутов