

Чтобы не стать жертвой мошенников рекомендуем вам ознакомиться с данной статьей.

В очередной раз сотрудниками Отдела МВД России по Крыловскому району проводятся профилактические мероприятия, направленные на борьбу с мошенниками. В последнее время резко возросли проявления мошенничеств, и борьба с этим видом преступлений обострилась. На территории нашего района ежемесячно регистрируются факты телефонного и интернет мошенничества.

Мошенничество все больше приобретает новые свойства, оно становится особым видом информационного воздействия на человеческую психику.

Данный вид преступного посягательства относится к категории технически сложных по замыслу и исполнению преступлений. Для его осуществления преступники часто объединяются в группы с четким распределением ролей в процессе подготовки и реализации преступного замысла. Организаторы и исполнители нередко обладают знаниями в области психологии.

Чтобы не стать жертвами мошенников, сотрудники полиции еще раз обращают Ваше внимание на ситуации, которые должны Вас насторожить.

Одним из наиболее распространенных способов совершения мошеннических действий является, так называемое, **телефонное мошенничество**, Вам звонят с незнакомого номера, в основном это номера стационарных телефонов г. Москвы и Московской области (8499, 8495) и представляются сотрудниками правоохранительных органов, либо ревизором. Далее лже-сотрудник сообщает, что распространители биологических активных добавок, у которых приобретали товар, арестован и Вам полагается

компенсация в размере от 300 000 до 5 000 000 рублей, в обмен на перевод «незначительной» денежной суммы на расчетные счета, которые необходимы для оплаты комиссии, страховки, налога, оформление документов, перевод денежных средств и иных услуг. В дальнейшем, заинтересованные граждане в «получении больших денег», выдают мошенникам ещё более крупные денежные суммы.

Сотрудники полиции Отдела МВД России по Крыловскому району предупреждают: компенсация за биологически активные добавки – одна из самых распространенных схем обмана граждан. Чтобы не попасться на уловки мошенников, не совершайте действия, на которые Вам указывает неизвестное лицо, позвонившее по телефону. В случае поступления предложений от имени правоохранительных органов о получении каких-либо компенсаций за приобретенные товары и услуги, не спешите называть данные своей банковской карты или переводить денежные средства на незнакомые счета в целях обогащения. В подобных ситуациях уточните информацию лично, посоветуйтесь с родственниками.

Новый способ мошенничества: Дистанционные аферисты похищают деньги с помощью приложения

TeamViewer, QuickSupport

Очередным способом мошенничества, с помощью которого наживаются злоумышленники, является хищение денежных средств с банковских счетов с помощью удалённого доступа, через приложение TeamViewer, QuickSupport.

Мошенник звонит случайным людям и представляется банковским работником, но не требует раскрыть номер, срок действия и секретный код на карте. Даже наоборот — предупреждает, что эти сведения нельзя выдавать посторонним, чем повышает доверие

к себе. После чего, мошенник говорит потенциальной жертве о том, что банк якобы зафиксировал попытку несанкционированного вывода средств с её счета, или о том, что неизвестное лицо пытается оформить кредит, и в целях безопасности банк заблокировал эту операцию до тех пор, пока не получит подтверждение от клиента.

Далее лже сотрудник банка, просит установить программу «TeamViewer «QuickSupport» (или другое приложение похожее по функционалу), которая позволяет получить удалённый доступ к чужому смартфону или компьютеру. После чего мошенники просят сообщить код, тем самым получая полный контроль над телефоном жертвы и его функционалом с возможностью совершения мошеннических операций. С помощью программ «TeamViewer и «QuickSupport» мошенник получает полный доступ к смартфону жертвы и может перехватывать SMS-сообщения от банка и различных онлайн-сервисов, воспользоваться личным кабинетом «мобильного банка» и вывести денежные средства на подставной счёт, а также без ведома потерпевшего оформить потребительский кредит. При этом ему даже не требуется заражать смартфон вирусом или выпытывать конфиденциальную информацию.

Доказать несанкционированный доступ к банковскому счёту в данном случае очень сложно, поскольку фактически его не было. Потерпевшие сами по своей воле предоставляют мошенникам возможность дистанционно наблюдать за происходящим на экране своего смартфона, запускать любые приложения и посещать любые сайты. Другое дело, что потерпевшие явно не осознавали, к чему это может привести. На такие уловки могут попасться люди старшего поколения, а также те, кто далёк от мира высоких технологий и не знает обо всех возможностях программ, с помощью которых можно удалённо управлять устройствами.

Чтобы не стать жертвой мошенничества и не потерять свои денежные средства следуйте следующим правилам:

1. Игнорируйте звонки с абонентских номеров (8495, 8499, 8800) с информацией о том, что Вам положена какая – либо денежная компенсация в обмен на перевод денежных средств на расчётные счета, либо о том, что с банковского счёта неизвестное лицо пытается осуществить перевод денежных средств.
2. Не общайтесь с посторонними людьми по телефону и не сообщайте номера своих банковских карт, коды доступа, смс - сообщения которые поступают к Вам на телефон иным лицам.
3. Перед тем, как перевести денежные средства на номер сотового телефона лица, которое сообщает Вам, что он Ваш родственник попал в трудную ситуацию, прервите разговор и позвоните родственникам, узнайте действительно ли они в тяжелой ситуации. Если сообщают, что родственник в полиции, позвоните в отделение полиции в дежурную часть и узнайте находится ли в данном отделении Ваш родственник.

4. Если Вам сообщили, что Ваша карта заблокирована, обращайтесь в отделение Сбербанка к оператору, не выполняйте указания человека, представившегося оператором.

5. Не пользуйтесь телефоном, на который подключен «Мобильный банк» для выхода в интернет, т.к. Ваш телефон может быть заражен вирусом (даже при наличии современных антивирусных программ), который в дальнейшем без Вашего ведома переведет.

Если Вы или Ваши близкие стали жертвами мошенников, или Вы подозреваете, что в отношении Вас планируется противоправные действия – незамедлительно сообщите об этом в дежурную часть Отдела МВД России по Крыловскому району по телефонам: **32 – 6 – 67, 31- 6 -40, 31 – 2 – 02 или 02.**