**КАК ЗАЩИТИТЬСЯ ОТ ДИСТАНЦИОННОГО МОШЕНИЧЕСТВО**

По-прежнему одной из самых злободневных тем в сфере борьбы с преступностью является защита населения от так называемого «дистанционного» или «телефонного» мошенничества.

С попытками совершения в отношении себя таких преступлений, столкнулся практически каждый человек, пользующийся телефонной связью.

Несмотря на принимаемые правоохранительными органами усилия по раскрытию таких преступлений, а также на проводимую с населением разъяснительную работу, количество пострадавших граждан продолжает расти.

Способы и тактика совершения хищений постоянно совершенствуется, преступниками активно используются результаты технологического процесса, в том числе специальные технические и программные средства, а также методы «социальной инженерии».

Мошенники могут представиться сотрудниками банка и сообщить, что организация заблокировала счёт, начислила штраф за кредит или по карте проведена подозрительная операция. Представиться сотрудниками полиции, ФСБ, прокуратуры и запугать уголовным делом или сообщить о попавшем в беду родственнике.

Одной из распространенных уловок преступников, которой вводят в заблуждение граждан, является сообщение о необходимости отмены заявки на получение кредита, якобы уже поданной в банк от имени потерпевшего, которая сопровождается последующим «возвратом» денег, полученных в кредит, их переводом на «безопасный счет».

Могут применяться и более «банальные» предлоги, например звонки под видом сотрудников Пенсионного фонда, Налоговой службы, Госуслуг.

Общим является то, что мошенники, как правило, нагнетают ситуацию, торопят, пытаясь ввести жертву в стрессовое состояние, заставить действовать необдуманно, поспешно, запугивая возбуждением уголовного дела, привлечением к ответственности близкого родственника, возможностью оформления мошенниками кредита, хищения денежных средств на крупную сумму, отменой льгот, выплат, блокировкой сим-карты и так далее.

В таком состоянии человек может поделиться с преступниками конфиденциальной информацией или перевести деньги на счёт обманщиков.

В ряде случаев граждан убеждают скачать и установить программное обеспечение для удаленного управления устройством, что позволяет мошенникам получить доступ к устройствам потерпевшего и использовать в преступных целях информацию о состоянии счетов, реквизитах карт, направить заявки на получение кредитов в банковские и микрофинансовые учреждения, осуществить вывод денежных средств со счетов посредством онлайн-банкинга.

Установка вредоносной программы может быть осуществлена жертвой и не осознанно, когда злоумышленник в процессе разговора просто просит перейти по ссылке, пришедшей в сообщении…

Действуя в группе, преступники заверяют граждан в важности четкого выполнения поступающих указаний для сохранения денег на счетах, гарантированного «возвращения» заемных денег, оказания помощи правоохранителям в изобличении преступников из числа банковских служащих.

Как правило, общение спустя непродолжительное время переводится в один из интернет-мессенджеров, по преимуществу WhatsApp.

Во избежание существенных финансовых потерь ни в коем случае не следует устанавливать на мобильные устройства, персональные компьютеры программы удаленного доступа, сообщать коды доступа ( это могут быть коды для доступа к личному кабинету у банка, мобильного оператора, Госуслуг, подтверждение переадресации входящих сообщений и т.д.) не важно, к мобильному вести общение с незнакомыми людьми, кем бы они не представлялись, по мобильному телефону и в мессенджере.

Необходимо иметь ввиду, что такую же опасность, как сообщение кодов доступа в личный кабинет банка несет предоставление кодов доступа к личным кабинетам мобильного оператора, порталу Госуслуг и т.д.

Так, одним из способов совершения мошенничества является получение доступа к личному кабинету у мобильного оператора (под предлогом необходимости подтверждения участия в рекламной акции, связанной с освобождением от абонентской платы, предоставлением дополнительных бонусов и т.п.) и оформления виртуальной Sim-карты.

Получив доступ к управлению абонентским номером мобильного оператора преступники в течение короткого времени получают доступ и к личному кабинету потерпевшего в кредитной организации, оформляют кредит и выводят денежные средства со счета.

При получении информации о незаконном обращении за кредитом следует незамедлительно в одностороннем порядке прекратить разговор, переписку, после чего самостоятельно сообщить о произошедшем в банк, обслуживающий счет, по телефонам «горячих линий» и в правоохранительные органы.

Аналогичным образом следует поступать в случае поступления подозрительных звонков от имени сотрудников правоохранительных органов и иных лиц, предлагающих передать денежные средства для урегулирования вопроса с попавшим в беду близким человеком, сообщить какие-либо коды доступа, пароли и прочее: прервать разговор и самостоятельно связаться с родственником (банком, мобильным оператором, территориальным отделом полиции и т.д.).  ​​

Опасность представляет и просто утрата контроля за своим мобильным телефоном или Sim-картой, с которой осуществлялась, например, регистрация личного кабинета в банке.

В этом случае лучше незамедлительно предупредить соответствующий банк по «горячей линии» о возможных мошеннических действиях и заменить Sim-карту в офисе мобильного оператора.

Нужно отметить, что в случаях, когда хищение денежных средств уже произошло, банковские и микрофинансовые организации при обращении граждан, ставших жертвами мошенников, как правило, отказываются признавать заключенные от их имени договоры недействительными, заявляя о нарушении требований безопасности со стороны самих граждан и отсутствии вины со стороны банка (микрофинансовой организации), после чего начинают взыскивать задолженность с граждан в общем порядке.

Выиграть спор в суде, несмотря на наличие значительного количества положительных примеров, удается далеко не всегда.

Способы мошенничества постоянно совершенствуются, чтобы не стать их жертвой необходимо проявлять постоянную осмотрительность, а также регулярно напоминать о ней с своим близким, в особенности, людям пожилого возраста и детям.

Прокурор Солецкого района

советник юстиции Ю.В. Костюков