

Наиболее распространенные способы мошенничества с применением информационно-телекоммуникационных технологий

В условиях современного мира разновидность преступлений с использованием IT-технологий, весьма обширна. Такие преступления тщательно спланированы и, как правило, совершаются подготовленной организованной преступной группой на протяжении длительного периода времени.

Вот наиболее распространенные из них.

Злоумышленники, доподлинно зная о том, что их жертва трудоустроена в какой-либо организации, создают клон страницы в социальной сети (ВКонтакте, Telegram, Whatsapp) руководителя данной организации, после чего от его лица сообщают гражданину о якобы проводимой в их организации проверки ФСБ России факта перечисления сотрудниками организации денежных средств в поддержку Вооруженных Сил Украины.

После сообщения данного факта жертве непременно звонят якобы сотрудники ФСБ России и сообщают, что с их банковских счетов осуществляются переводы денежных средств на нужды Вооруженных Сил Украины.

Патриотически-настроенные граждане, думая о том, что их деньги могут оказаться в руках противника, выполняют все указания мошенников.

Для того, чтобы не стать жертвой такой схемы мошенничества, следует немедленно прекратить телефонный разговор, уведомить руководителя о получении указаний от его лица через социальную сеть, предупредить других сотрудников об этой ситуации. При необходимости через приложение банка заблокировать доступ к своим банковским счетам и обратиться в органы полиции.

Также мошенниками используется следующая схема: гражданину в социальной сети или интернет-мессенджере (ВКонтакте, Telegram, WhatsUp) приходит сообщение от клона профиля знакомого ему лица с текстовым сообщением «Это твои фотографии?/Это ты на видео?/Ты знаешь этого человека?» с приложением ссылки или стороннего файла любого другого формата. Текст сообщения может варьироваться. В любом случае содержание такого сообщения направлено на побуждении интереса у лица к открытию и прочтению сообщения.

При последующем открытии приложенной ссылки или стороннего файла происходит автоматическое скачивание вредоносного приложения, которое предоставляет мошенникам полный дистанционный доступ к мобильному устройству гражданина, что и позволяет в последующем осуществить хищение принадлежащих ему денежных средств.

Чтобы обезопасить себя от такого типа мошенничества следует помнить, что открывать диалоговое окно с приложенным файлом или ссылкой безопасно, но в последующем следует детально изучить полученное сообщение: установить, является ли профиль отправителя «подлинным», проверить контактные данные, обратить внимание на отсутствие в диалоге иных сообщений и медиа-файлов; обратить внимание на текст ссылки и формат приложенного файла. Следует остерегаться форматов «exe».

Также все большую популярность приобретает мошенничество в популярных среди детей онлайн играх, примером служит игра Roblox (роблокс). В ходе игры детям предлагается подписаться на страницу в социальной сети Телеграмм, где разыгрывается пополнение игрового счета. Для перечисления выигрыша, злоумышленники просят ребенка сфотографировать банковское приложение в телефоне родителей (сфотографировать банковскую карту, осуществить перевод денежных средств через приложение банка и пр.), требуют это сделать незамедлительно, объясняя тем, что приз скоро исчезнет.

Родителям важно защитить детей от мошенников. Необходимо проверять приложения, которые

использует ребенок, разговаривать с ним об угрозах в сети и правилах безопасного поведения в интернете. Необходимо объяснить ребенку, что вводить данные банковских карт или делиться иной личной информацией в интернете нельзя.