

ПРОКУРАТУРА ИНФОРМИРУЕТ

население Куйтунского района

о мерах безопасности при совершении банковских операций по картам/счетам, а также о предупреждении совершения преступлений с использованием злоумышленниками информационно-коммуникационных технологий

С каждым днем всё актуальнее становятся вопросы, связанные с хищением, совершенном с использованием современных информационно-коммуникационных технологий.

В настоящее время появились и распространяются следующие виды мошеннических действий:

1. Мошенничество под предлогом инвестирования в ценные бумаги и криптовалюту (разновидность цифровой валюты, учитываемой в децентрализованной платежной системе). При таком посягательстве злоумышленники представляются финансовыми брокерами и заманивают граждан «исключительными» (выгодными) предложениями, возможностью получения высокого дохода, используя названия крупных нефте-газодобывающих компаний и холдингов (например, «Binance», Газпроминвестиции, ТинькоффИнвест), вынуждают потерпевшего вносить крупные суммы денежных средств без возможности их дальнейшего вывода (получения).

Как в этой схеме совершения преступления, так и в последующих, потерпевшими могут стать все категории граждан независимо от пола, возраста, образования, экономического, национального, социального статуса.

2. Злоумышленник представляется сотрудником кредитно-финансовых учреждений и (или) правоохранительных органов. Используя методы психологического манипулирования и пользуясь доверчивостью, он вынуждает потерпевшего сообщать персональные данные, сведения о финансовом состоянии, наличии автотранспорта в собственности. Затем, находясь под психологическим воздействием мошенника, потерпевший переводит денежные средства на якобы безопасные расчетные счета. В отдельных случаях переводятся средства, вырученные от срочной продажи автотранспорта или недвижимости. Причем сделку по срочной продаже имущества могут организовать сами мошенники.

3. Мошенничество, совершаемое под предлогом взломанной учетной записи на Едином портале государственных и муниципальных услуг (далее - портал «Госуслуги»). В этом случае злоумышленник, маскируясь под представителя оператора связи, убеждает потенциальную жертву посягательства, что срок действия sim-карты для использования мобильной связи истекает. Для продления ее работы необходимо сообщить код из присылаемого SMS-сообщения. На самом деле это оказывается код для входа в личный кабинет на портале «Госуслуги». После того как мошенники получают код, они входят в учетную запись, меняют контрольный вопрос и оставляют сообщение о блокировке аккаунта и необходимости позвонить по указанному номеру. Войдя в учетную запись, мошенники могут оформить кредит на потерпевшего, получить его налоговый вычет, продать данные о нем или же собрать информацию о гражданине с целью дальнейшего так называемого «адресного психологического давления» - процесса

сбора данных, предварительной подготовки и использования эмоциональных триггеров, направленных на конкретного человека (событий, вызывающих у него автоматическую (иногда неконтролируемую) эмоциональную или поведенческую реакцию)

4. Звонки или сообщения от знакомых.

Еще одна тактика злоумышленников – рассылка сообщений с просьбой одолжить денег близким или друзьям. Порой в своих сценариях мошенники заходят и дальше – играют на чувствах жертвы и сообщают, что ее родственник попал в беду. Если раньше аферистам приходилось разыгрывать театральный спектакль, подделывая голос, то теперь за них это делает искусственный интеллект. Злоумышленники взламывают аккаунт пользователя, скачивают голосовые сообщения и на их основе генерируют монолог для дальнейшего обмана.

Существует и другой «безобидный» сценарий – просьба проголосовать за детей или племянников в детском конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который откроет им доступ к вашему гаджету.

Не открывайте и не устанавливайте файлы с расширением .apk и другие подозрительные вложения, полученные через электронные сообщения или мессенджеры.

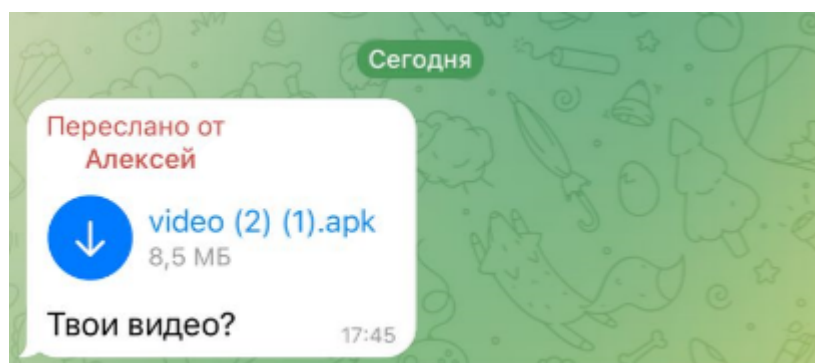
Чаще всего злоумышленники направляют файлы, сопровождая их вопросом: «Это ты на видео?», также слово «видео» в разных вариациях используется в названии файла.

При открытии файла происходит установка приложения, после чего устройство может быть заражено трояном Mamont, считывающим push-уведомления, СМС сообщения и фотографии из галереи.

Кроме того, троян может автоматически пересылать данный файл всем контактам в мессенджере.

Регулярно обновляйте антивирусные программы и операционную систему вашего мобильного устройства до последних версий.

Конечная цель злоумышленников - получение доступа к платежным средствам, однако персональные данные и любая информация со смартфона также может быть использована в противоправных целях.



Не переходите по неизвестным ссылкам, даже если получили их от близких или знакомых. Договоритесь с родственниками о пароле или секретном вопросе, который нужно назвать, если разговор кажется подозрительным. Такой шаг поможет раскусить намерения мошенника.

5. Оплата услуг по фейковому QR-коду.

Сегодня, чтобы получить какую-либо услугу или оплатить товар, достаточно навести камеру на QR-код. Например, им можно воспользоваться, чтобы взять в аренду самокат или портативное зарядное устройство для гаджета. Правда, вместо прогулки с ветерком и заряженного аккумулятора телефона можно получить пустой банковский счет. Дело в том, что такой QR-код ведет не на официальный сайт сервиса, а на поддельный ресурс, через который аферисты крадут деньги и данные карты.

Оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета.

При совершении мошеннических действий потерпевшему следует незамедлительно обратиться в правоохранительные органы и написать заявление о свершившемся противоправном деянии, либо позвонить с мобильного телефона по номерам 102 и 112, с городского телефона по номерам 02 и 102.