Информация
о появлении новых способов совершения преступлений с использованием информационно-телекоммуникационных технологий

ГУ МВД России по Челябинской области информирует о появлении новых способах совершения дистанционных мошенничеств:

1. Распространение электронных писем на почту, приходящих от так называемого «центра обмена сообщениями хостинга веб-почты» - от несуществующей организации. Авторы рассылки сообщают, что обновляют некую базу и удаляют все неиспользуемые учетные записи. Они настоятельно рекомендуют подтвердить электронную почту и обновить данные для того, чтобы знать, что аккаунт активен и его не будут удалять. При этом не используются вредоносные программы и фишинговые сайты, необходимую мошенникам информацию (имя, фамилию, логин и пароль) просят прислать ответным сообщением. Таким образом мошенники получают доступ к личным данным граждан.

2. Активизация подделки мошенниками банковских приложений, например именуемых как «Сбер 2.0» и «Поддержка Сбербанка». Злоумышленники звонят клиентам якобы от имени сотрудника «Сбера» и рекомендуют (убеждают) установить на современные средства коммуникации (мобильные телефоны) приложения «Сбер 2.0» или «Поддержка Сбербанка». На самом деле под видом этих приложений распространяются программы для удаленного доступа к устройствам. Если пользователь установит одно из таких приложений, мошенники могут похитить его личную информацию и деньги с банковских карт.

3. Обманные действия под видом представителя оператора мобильной связи. Злоумышленники, маскируясь под сотрудника оператора связи, убеждают потенциальную жертву, что срок действия sim-карты мобильного телефона истек. Для продления ее работы необходимо сообщить код из сообщения. После получения кода преступники подключают переадресацию звонков и SMS на другой номер и получают доступ к онлайн-банку, социальным интернет-сетям и мессенджерам жертвы для входа по номеру телефона.

4. Использование новых функций интернет-приложений («мессенжеров») для совершения преступлений. Появилась новая функция в телеграм-каналах - возможность публиковать изображения - так называемые «сторис». Для этого необходимо получить определенное количество голосов («бустов»). В связи с этим появились автоматические чат-боты в «мессенджерах», предлагающие купить «бусты» в больших количествах. Вводить данные банковской карты при этом не требуется, злоумышленники просят выслать деньги обычным переводом. Пользователь переводит деньги, но не получает никаких гарантий, при этом у чат-бота отсутствует форма обратной связи.

5. Предложения по установке мобильного приложения с целью проверки качества работы смартфона. Фиктивная служба поддержки банка присылает ссылку на фишинговый сайт и предлагает подключить услугу безопасности смартфона. После того, как клиент соглашается на подключение и устанавливает на устройство мобильное приложение, мошенники получают доступ к онлайн-банку и похищают денежные средства.

6. Звонки злоумышленников якобы от имени руководства компаний и организаций. Представляясь генеральным директором, мошенники предупреждают служащих, что им скоро поступит телефонный звонок от представителя курирующего эти компании Министерства. При этом, в «мессенджерах» используются аккаунты с реальными фотографиями и данными руководителей (фамилия, имя, отчество). Далее действительно поступает звонок, в ходе разговора мошенники под различным предлогом получают конфиденциальную информацию, с целью совершения мошеннических действий.

ГУ МВД России по Челябинской области