УПРАВЛЕНИЕ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО СИБИРСКОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ

ПАМЯТКА
ПО ПРОФИЛАКТИКЕ
КИБЕРМОШЕННИЧЕСТВА

Потерпевшими от киберпреступлений являются граждане абсолютно всех категорий, включая как социально-незащищенные слои населения (инвалиды, пенсионеры, несовершеннолетние), так и люди, занимающие руководящие посты в организациях (предприятиях) всех форм собственности, имеющие несколько высших образований.

В ходе совершения преступлений злоумышленники используют звонки с номеров, визуально приближенных к номерам телефонов правоохранительных органов, служб банков (например, звонки на WhatsApp с номера +900, 9OO, тогда как официальный номер Сбербанка 900).

На сегодняшний день набирает популярность среди мошенников реализация преступных схем с использованием искусственного интеллекта. Используемые мошенниками схемы постоянно меняются, «подстраиваясь» под общественно-политическую обстановку, значимые события в государстве.

Так, в Сибирском федеральном округе в 2024 году совершено 15 437 краж и 46 925 фактов мошенничества с использованием информационно-телекоммуникационных технологий (компьютерная техника и средств мобильной связи).

Вашему вниманию представлены наиболее распространенные способы совершения киберпреступлений.

Обман под видом предложений от известных компаний и «Подмена мерчанта (продавца)»

Злоумышленники создают фишинговые ресурсы для хищения данных и денежных средств, имитируя страницы крупных компаний, интернет-магазинов. Жертве предлагается приобрести товар, услугу по скидке или поучаствовать в акции. Для привлечения жертвы используют контекстную рекламу, рассылку в менеджерах.

Поддельные штрафы

Мошенники имитируют уведомления от органов исполнительной власти о якобы имеющихся штрафах, задолженностях. Соответствующие сведения направляют в адрес электронной почты и предлагаю произвести оплату перейдя по ссылке из фишингового письма. Рассчитывая заплатить штраф или погасить задолженность, жертва переходит по ссылке и вводит данные банковской карты в мошенническую форму оплаты.

Обман на площадках бесплатных объявлений (Avito и др.) и маркетплейсах

В большинстве случаев жертва сама входит в контакт с мошенниками в чате на сайте объявлений или маркетплейсах для покупки товара. В ходе общения злоумышленники предлагают продолжить переписку в мессенджере для уточнения деталей или доставки товара. Мошенники запрашивают у жертвы ФИО, адрес, номер телефона для заполнения формы доставки. Жертву вынуждают перейти по ссылке на заранее сгенерированный фишинговый ресурс, который имитирует официальные страницы курьерских служб, после введения банковских реквизитов списываются средства.

Криптоскам, псевдоброкеры,финансовые пирамиды

Широко получившая последнее время схема, в результате использования которой причиняется наиболее крупный ущерб – заработок на бирже, заманивание прибыльными инвестициями, в том числе в криптосфере. Преступниками создается максимальная видимость того, что общение происходит с представителями крупной инвестиционной площадки, их сайты имеют видимое сходство с банковскими организациями (например, Газпром-инвестиции, РБК-инвестиции, Тинькофф-инвестиции и т.д.), назначается личный брокер, общение с которым может осуществляться даже посредством видеозвонков. Под их руководством создается якобы личный кабинет на торговой площадке, в котором отображаются все внесенные денежные средства, и прибыль. Однако их дальнейший вывод невозможен.

Результат – списание денег со счетов, взятие кредита.

Рассылка налоговых писем о выявлении подозрительных транзакций и активности налогоплательщика

В поддельном сообщении предлагается пройти дополнительную проверку и предоставить сведения по запросу налоговой службы. Так мошенники могут запросить кассовые документы, счета-фактуры, отчетные документы. Далее для прохождения проверки предлагается обратиться к указанному в письме инспектору под угрозой блокировки счетов налогоплательщика. Важно помнить, что налоговая не рассылает такого рода письма и не имеет отношения к ним, такие письма открывать не рекомендуется, как и переходить по ссылкам.

Удаленное управление устройством под видом технической поддержки

Злоумышленники представляются сотрудниками технической поддержки банка, сообщают, что зафиксирована попытка мошеннических манипуляций с картой жертвы. Убеждают в необходимости сохранить денежные средства и защитить банковское приложение. Жертва соглашается установить на смартфон приложение удаленного управления и разрешить подключение к устройству «сотруднику банка». Мошенники могут направлять файл с программой удаленного управления напрямую клиенту через мессенджер или предлагают ее скачать в Google Play или App Store. Если удалось убедить жертву установить программу удаленного доступа, мошенники просят зайти в мобильное приложение банка и проверить сохранность средств, а затем положить устройство экраном вниз и подождать пока сотрудники настроят приложение или переведут средства на «безопасный счет».

Фиктивные социальные выплаты и компенсации

На специализированных теневых площадках в сети Интернет злоумышленники приобретают похищенные базы данных граждан (ФИО, даты рождения, адрес и пр.), обманутых ранее при покупке БАДов, поддельных лекарств, турпутевок. Используя эту информацию, мошенники обзванивают жертв и представляются сотрудниками Пенсионного фонда России, Росздравнадзора, банков, социальных служб. Жертве предлагается получить компенсацию или выплаты, для получения которых необходимо сообщить реквизиты банковской карты для поступления средств.

«Ошибочный» перевод

Мошенник отправляет деньги на счет жертве, а затем звонит и убеждает вернуть их. В это время обращается в банк, чтобы отменить свой перевод до наступления момента безотзывности.

Наиболее распространенные схемы киберпреступлений

Обман под видом службы безопасности

Злоумышленники представляются представителями службы безопасности банка, Центрального банка России, Росфинмониторинга либо правоохранительного органа и сообщают, что мошенники с использованием персональных данных потерпевшего оформляют кредиты в различных банках и для того, чтобы предотвратить хищение денег с банковского счета необходимо личные сбережения срочно перевести на «безопасные счета». В ходе дальнейшего общения потерпевшему сообщают о необходимости оформления кредитов и их перевода. Следует отметить, что общение потерпевшего со злоумышленниками является длительным, в некоторых случаях осуществляется в течение нескольких месяцев, используется как телефонная связь, так и общение посредством мессенджеров (Ватсап, Вайбер, Телеграм и т.д.). Для достоверности мошенники могут присылать жертве поддельные документы от имени банка и других организаций. Следует помнить, что «безопасных счетов» не существует, а представители Центрального Банка России не осуществляют работу с физическими лицами.

Злоумышленники «продают» Вашу квартиру или машину

Злоумышленники в ходе телефонного разговора представляются представителями службы безопасности коммерческого банка, Госуслуг, Центрального банка России либо правоохранительного органа. Сообщают о том, что персональные данные с личного кабинета утекли и теперь преступники могут от Вашего имени продать квартиру, машину, используя электронно-цифровую подпись. В целях защиты убеждают срочно продать имущество и перевести деньги на «защищенный канал», «безопасный счет», «резервную ячейку».

СМС от работодателя

Потерпевшему поступает смс сообщение или сообщение в мессенджере от работодателя (возможно использование подменных номеров) о том, что с ним в ближайшее время свяжется сотрудник ФСБ или иной организации, с которым ему следует пообщаться. После этого звонит мошенник, представляется сотрудник с именем, указанным руководителем, и сообщает о попытках перевода личных сбережений на иностранные счета/финансирование территоризма/Украины и т.п. В целях пресечения преступных операций потерпевшего убеждают прервать транзакции путем перевода денег (личных накоплений или путем взятия кредита) на счет, указанный злоумышленниками.

Привлечение к вымышленному расследованию

Мошенники представляются сотрудниками правоохранительных органов (полиция, ФСБ, прокуратура) и сообщают, что в отношении Вас возбуждено уголовное дело в связи с финансированием экстремисткой, террористической деятельности, поскольку с Вашего банковского счета осуществлен перевод денежных средств в недружественное государство. Либо сообщают, что к ним обратились из службы безопасности банка по поводу приостановленной попытки оформления на имя жертвы кредита. В ходе общения мошенники могут присылать якобы фото удостоверений, повесток, постановлений о возбуждении уголовного дела, подписок о неразглашении следственной тайны и т.д. Злоумышленники могут обращаться к жертве в строгом, практически, командном тоне, иногда доходящим до грубости, нередко используют юридические термины.

Обман с использованием QR-кода

Жертву убеждают, что ее средства находятся в опасности и указывают на необходимость их внести на «безопасный счет». Мошенники направляют к банкомату с функцией приема денежных средств по QR-коду, после чего просят прислать им через мессенджер сгенерированный QR-код для активации «безопасного счета». Полученный QR-код злоумышленники сканируют в своем банковском приложении. Жертва, находясь в заблуждении, собственноручно вносит средства на счета дропов через банкомат.

Хищение денежных средств через систему быстрых платежей (СБП)

Например, покупатель на сайте в сети Интернет оставляет заявку на приобретение товара. После чего ему поступает звонок якобы от сотрудника магазина, предлагается скидка на товар, но только при условии оплаты через СБП или QR-коду, затем злоумышленник присылает в мессенджер ссылку, ведущую на страницу с формой оплаты по QR-коду. Покупатель подтверждает платеж и денежные средства поступают на счет мошенника. Важно в такой ситуации связаться со службой поддержки онлайн-магазина, через официальный сайт или приложение. Не сохранять для оплаты в личных кабинетах банковские карты, при возможности заведите отдельную карту для оплаты покупок онлайн.

Звонок мобильного оператора

Злоумышленник под видом мобильного оператора сообщает, что срок действия вашей сим-карты истек либо истекает, а для его продления необходимо сообщить код, который поступит в смс либо пройти по ссылке, в противном случае сим-карта будет заблокирована. Важно знать, что у сим-карты нет срока действия, сотовые операторы перевыпускают сим-карты только по просьбе потребителей в случае физического износа, потери,

необходимости получения сим - карты другого формата. Выполнив требования мошенников и сообщив код из смс, либо пройдя по ссылке Вы отдаете в руки злоумышленников доступ в свой личный кабинет на сайте оператора связи, после чего мошенники имеют возможность устанавливать переадресацию сообщений на нужный им номер, что позволит сменить пароль от мобильного банка и похитить денежные средства. Вторая разновидность таких преступлений – получение злоумышленником кода из смс, и последующего доступа к аккаунту «госуслуг» для оформления заявок на кредиты в банках.

«Родственник в беде»

Злоумышленник представляется родственником потерпевшего, знакомым либо представителем правоохранительного органа. При этом просит перевести денежные средства, например, для дачи взятки должностному лицу за урегулирование проблем с ДТП, оплаты медобслуживания ввиду обнаружения тяжелого заболевания, и др. Наиболее подвержены данному виду преступлений пожилые граждане. Звонки совершаются в основном рано утром или поздно вечером, когда жертвы менее склонны к критическому мышлению.

Хищения с использованием искусственного интеллекта

Мошенниками производится взлом либо копирование аккаунта пользователя в мессенджерах Ватсап, Вайбер, Телеграмм, социальных сетей Вконтакте и дальнейшее направление сгенерированных искусственным интеллектом (нейросетью) голосовых сообщений от имени потерпевшего, которое полностью копирует его голос, используя при этом ранее отправленные сообщения владельца аккаунта. А дальше все по типичной схеме – просьба одолжить взаймы, фото банковской карты для перевода денежных средств. В данной ситуации важно убедиться, что вы общаетесь именно с Вашим знакомым путем звонка по мобильной сети. Сделав это, Вы обезопасите себя и предупредите знакомого о том, что от его имени действуют мошенники. Для того, чтобы не потерять контроль над Вашим аккаунтом никогда не переходите по незнакомым ссылкам, не скачивайте программы из неподтвержденных источников, используйте двухфакторную аутентификацию аккаунтов. Будьте максимально внимательны, поскольку следующим этапом использования искусственного интеллекта может явиться генерация видеоизображений и рассылка видеосообщений от имени родных, коллег, знакомых и т.д.

Сдача налоговых деклараций и справок о доходах

Звонившие представляются сотрудниками Госуслуг, управления по делам Президента РФ, сообщают, что в рамках декларационной компании проверяют персональные данные лиц, сдавших налоговые декларации либо декларации о доходах. Со слов преступников – для подтверждения следует назвать паспортные данные и код из СМС.