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.

Злоумышленниками используются изощренные способы «выманивая» денежных средств, для чего используются различные «легенды», посредством изложения которых оказывается психологическое воздействие на граждан, которые под его воздействием выполняют все команды злоумышленников. Многие из потерпевших в дальнейшем в ходе общения с сотрудниками правоохранительных органов сообщают, что действовали «под гипнозом», в результате профессиональной манипуляции со стороны преступников.

В ходе совершения преступлений злоумышленники используют звонки с номеров, визуально приближенных к номерам телефонов правоохранительных органов, служб банков (например звонки на Вайбер с номера +900, 9ОО, тогда как официальный номер Сбербанка 900 и т.д.), представляются официальными лицами.

Наиболее распространенными способами преступлений на сегодняшний день являются:

1. СМС от работодателя.

Потерпевшему поступает смс сообщение или сообщение в мессенджере от работодателя. О том, что с ним в ближайшее время свяжется сотрудник ФСБ или иной организации, следует с ним пообщаться.

После этого звонит сотрудник с именем указанным руководителем и сообщает о попытках перевода личных сбережений на иностранные счета / финансирование территоризма / украины и тп.

В целях пресечения преступных операций потерпевшего убеждают прервать транзакции путем перевода денег (личных накоплений или путем взятия кредита) на счет, указанный злоумышленниками.

2. Злоумышленники «продают» Вашу квартиру или машину.

Звонившие представляются представителями службы безопасности коммерческого банка, Гос услуг, Центрального банка 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 его продать – перевести деньги на «защищенный канал», «безопасный счет», «резервную ячейку».

3. Перевод денег на «безопасный счет», якобы для их сохранности.

Звонившие представляются либо представителями службы безопасности коммерческого банка, Центрального банка 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. Также зарегистрированы случаи продажи недвижимости и перевода мошенникам вырученных средств.

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.).

Еще одна разновидность преступной схемы – когда **звонят якобы сотрудники правоохранительных органов 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.

В ходе общения злоумышленники могут присылать якобы фото удостоверений, повесток, постановлений о возбуждении уголовного дела, подписок о неразглашении следственной тайны и т.д. Нужно быть предельно внимательными, не поддаваться манипуляциям и проверять сообщаемую информацию,

Кроме того, следует помнить, что «безопасных счетов» не существует, а представители Центрального Банка не осуществляют работу с физическими лицами.

4. Звонок злоумышленника **под видом мобильных операторов, которые сообщают, 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 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 в результате сообщения кода из смс доступа к аккаунту «госуслуг», дальнейшее оформление заявок на кредиты в банках, получение к персональным данным, таким как сведения о доходах, наличие банковских счетов и т.д.

5. Сдача налоговых деклараций и справок о доходах.

Звонившие представляются сотрудниками Госуслуг, управления по делам президента, 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.

Результат – списание денег со счетов, взятие кредита.

6. **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 Ваших 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.

7. **Хищение денежных средств через систему быстрых платежей (СБП).**

Например, покупатель на сайте оставляет заявку на приобретение товара, 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.

8. Широко получившая последнее время схема, в результате использования которой причиняется наиболее крупный ущерб – **заработок на бирже, заманивание прибыльными инвестициями**. Преступниками создается максимальная видимость того, что общение происходит с представителями крупной инвестиционной площадки, их сайты имеют видимое сходство с банковскими организациями (например, Газпроминвестиции, 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.

Например, жительница г. Сосновоборск в сети интернет увидела псевдорекламу «Газпромбанка» о дополнительном заработке, ввела свои паспортные данные на сайте. спустя несколько дней с ней связался сотрудник торговой компании и рассказал о возможном росте финансовых накоплений в ходе торгов и дальнейшего вывода прибыли. Заинтересовавшись, женщина установила инвестиционную платформу и стала сотрудничать якобы с финансовым специалистом через приложение «скайп». Первоначально внесла депозит в размере 10 тыс, после чего увидела прибыль в размере 2 тыс, которые ей поступили на банковскую карту. Это придало веру в возможность зарабатывать. Обманутая женщина вносила личные денежные средства, которые получила путем оформления кредитов в различных банках, думая, что торгует газом, нефтью, серебром, акциями «Газпрома». В дальнейшем, при оформлении сделок, система стала выдавать ошибки. Лже-специалисты поясняли, что необходимо оформить страховку и ряд других финансовых манипуляций, однако работа на платформе была заблокирована. Действуя по инструкции мошенников, потерпевшая перевела более 6 млн. руб.

9. 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 ФНС не рассылает такого рода письма и не имеет отношения к ним, такие письма открывать не рекомендуется, как и переходить по ссылкам.

8. Схема «**Ваш родственник попал в ДТП**», наиболее подвержены данному виду преступлений пожилые граждане. Злоумышленник представляется либо родственником потерпевшего либо представителем правоохранительного органа и сообщает, что для освобождения от уголовной ответственности и наказания в виде лишения свободы срочно необходимо передать денежные средства.

ВАЖНО ЗНАТЬ!!!!

Используемые мошенниками схемы постоянно меняются, «подстраиваясь» под общественно-политическую обстановку, значимые события в государстве. Распространены также следующие способы:

- обман во время кампании по сдаче налоговых деклараций (поступление письма от злоумышленников на электронную почту от якобы сотрудников налоговой службы с требованием представить декларацию по специальной ссылке при переходе на которую необходимо ввести личные данные и реквизиты банковской карты якобы для идентификации налогоплательщика);

-хищение денег и имущества под предлогом обновления банкнот (звонок от мошенников с указанием о необходимости проверки подлинности банкнот Банка России, для чего убеждают установить стороннее приложение, посредством которого получают удаленный доступ к телефону жертвы; также используется поквартирный обход от якобы специалистов социальных служб, которые убеждают обменять денежные купюры на поддельные);

- использование ложных аккаунтов руководителей Банка России, правоохранительных органов, органов прокуратуры, содержащих реальные данные, взятые из открытых источников (фамилию, имя, отчество, фото);

- сообщение клиентам банков об утечке персональных данных;

- обещание помочь с компенсацией ранее похищенных денег;

- обмен кэшбека на рубли.

БУДЬТЕ БДИТЕЛЬНЫ!!!!!

@KRPRO_PRAVZN