Приложение №1

Информация для проведения лекции в трудовых коллективах по теме противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Несмотря на то, что органами внутренних дел Кузбасса на постоянной основе проводится комплексная работа по профилактике различных способов дистанционных преступлений, граждане по-прежнему попадаются на уловки злоумышленников.

Продолжают иметь актуальность хищения денежных средств граждан, совершенных с использованием информационно-телекоммуникационных технологий. Одновременно с развитием в данной сфере появляются и новые виды дистанционных преступлений, позволяющие обмануть и присвоить денежные средства граждан.

«Схема с обыском или уголовным делом»

Под различными предлогами мошенники устанавливают контакт с ребенком, выясняют его персональные данные, после чего направляют ему вредоносные ссылки и продолжают взаимодействие посредством телефонных звонков и сообщений в мессенджерах. В дальнейшем звонки продолжаются с других абонентских номеров, где мошенники представляются уже сотрудниками правоохранительных органов, поясняют, что ребенок прошел по сомнительной ссылке и начинают давление: пугают подростков, при этом поясняют, что родители, как соучастники, также будут привлечены к уголовной ответственности. Зачастую злоумышленники владеют персональными данными родителей – их именами, адресами и даже местом работы – что дополнительно усиливает воздействие на психику ребенка.

Цель аферы – добиться от ребенка доступа в квартиру. Для предварительной оценки ценных предметов, находящихся в квартире, мошенники просят показать квартиру по видеосвязи, называя это «добровольным онлайн обыском». Далее детей вынуждают оставить ключи от квартиры в заранее оговоренном тайном месте «для проведения обыска сотрудниками ФСБ», после чего принуждают под разными предлогами увести родителей из дома или сообщить мошенникам, когда они будут отсутствовать продолжительное время. В момент отсутствия, в квартиру проникает сообщник мошенников, совершая хищение ценного имущества. Иногда в таких схемах, если в квартире имеется сейф, у ребенка пытаются узнать пароль от сейфа, если ребенку он неизвестен, замки на нем в последующем спиливают.

Запомните:

1. Уголовная ответственность не может наступить за сам факт перехода по ссылке - это вымысел мошенников;

2. Правоохранительные органы (полиция, прокуратура, ФСБ) никогда не решают подобные вопросы посредством звонков несовершеннолетним и не просят их тайно обыскивать квартиру или передавать имущество;

3. Ребенку необходимо незамедлительно рассказывать взрослым о подобных случаях, а не пытаться действовать самостоятельно;

4. Ни при каких обстоятельствах нельзя доверять незнакомцам по телефону, передавать информацию, деньги или имущество, даже если «очень страшно»;

5. Если ребенок получил подобный звонок или сообщение, родителям необходимо попросить его немедленно прекратить общение с незнакомцем;

6. Родителям необходимо регулярно обсуждать с детьми правила безопасности (не переходить по ссылкам от незнакомцев в сети «Интернет», не сообщать личные данные и коды из смс-сообщений, не выполнять тайных поручений по просьбе неизвестных лиц).

Чат знакомств

Мошенник начинает переписку с жертвой в чат-боте (мобильном приложении, сайте) знакомств, добивается взаимной симпатии, предлагает встречу. После чего просит отправить геолокацию или отправляет ссылку для оплаты, например, «билета в кино». После того как жертва отправляет свою геолокацию (точку на карте) или переходит по ссылке для оплаты, поступает звонок, в котором злоумышленник представляется сотрудником правоохранительных органов и говорит: «Деньги ушли на поддержку ВСУ, а геолокацию использовали для подготовки атаки. Никому ничего не рассказывай. Или мы заведем уголовное дело». Иногда для шантажа мошенники, в ходе общения, выманивают личные фото.

Далее жертву начинают запугивать, требовать деньги, доступ к банковским счетам или предлагают выполнить опасное задание, чтобы, якобы, избежать наказания.

Запомните:

1. Необходимо немедленно прекращать подобные разговоры.

2. Не переходить по ссылкам, направленным малознакомыми людьми и не скачивать файлы.

3. Блокировать такие контакты в своем мобильном устройстве.

4. Проверять информацию альтернативным способом, особенно если речь, о личных данных.

Звонок от сотрудника банка

Злоумышленники звонят пожилым людям, представляются сотрудниками банка и утверждают, что пенсию автоматически переводят в цифровые рубли, и предлагают оформить отказ для сохранения привычных выплат. Для этого мошенники просят продиктовать код из СМС. Жертва не заметит, как продиктует комбинацию чисел из СМС-сообщения, не обратив внимание, что сообщение приходит от портала «Госуслуги», а в самом сообщении написано «Код восстановления доступа к учетной записи. Не сообщайте никому!». Следом, на жертву обрушается шквал звонков с портала «Госуслуги», «Росфинмониторинг» или правоохранительных органов. Мошенники утверждают, что в аккаунте жертвы уже хозяйничают преступники, оформляют кредит и переводят за границу, снимают денежные средства с банковских счетов, переоформляют на себя недвижимость, поэтому нужно подтвердить все заявки или снять накопления и перевести на безопасный счет.

Запомните:

1. Автоматического перевода пенсий в цифровые рубли не существует.
2. Способ получения выплат не меняется без личного заявления человека.
3. Любой запрос кода из сообщения является признаком обмана.
4. Если передали информацию, то немедленно свяжитесь с поддержкой портала «Госуслуги» и заблокируйте учетную запись.
5. Сотрудники банков никогда не потребуют конфиденциальных данных из СМС-сообщений, не потребуют действий с вашими финансами, не отправят к банкомату, чтобы перевести деньги.

ИИ-сервисы с вредоносным ПО

Злоумышленники маскируют шпионские программы под безобидные приложения: для подбора прически, макияжа, кулинарных рецептов. Человек скачивает файл по ссылке из интернета, а на устройство устанавливается ПО, дающее мошенникам удаленный доступ. Дальше они могут перехватывать СМС-сообщения, читать банковские уведомления, шантажировать или убеждать перевести деньги.

Запомните:

1. Не переходите по ссылкам, не заполняйте ничего на сторонних сайтах.
2. Проверяйте адрес сайта (ссылку сайта). Обратите внимание на наличие замка в адресном сроке браузера, который подтверждает зашифрованное соединение. Если вы видите «http://», а не «https://», это сигнализирует о возможной угрозе.

Обман вокруг цифрового рубля

После внедрения цифрового рубля мошенники стали рассылать сообщения, имитирующие официальные уведомления от Центрального Банка России или Госуслуг. В них пугают блокировкой счетов, если человек немедленно не конвертирует свои деньги в новую форму валюты. Чтобы спасти средства, жертву просят срочно закрыть счет и перевести все на «транзитный резервный счет», который на деле оказывается кошельком злоумышленников.

Запомните:

1. Цифровой рубль добровольный. Никто не обязан открывать цифровой кошелек. При этом никаких заявлений об отказе в МФЦ, банке или где-либо еще писать не нужно.

2. Кошелек открывается только лично – через мобильное приложение вашего банка, подключенного к платформе цифрового рубля. Автоматически счета никому не открываются, и сделать это за вас никто не может.

3. Принудительной конвертации нет и не планируется.

Оплата налогов (штрафов)

Злоумышленники связываются с человеком по телефону, в мессенджере или даже присылают поддельное письмо. Они представляются сотрудниками Федеральной налоговой службы) или иногда Федеральной службы судебных приставов. Жертве говорят, что за ней числится задолженность (иногда придумывают деталь – например, не уплачен налог с какого-то дохода или есть ошибка в декларации). Чтобы «исправить ситуацию», «специалист» просит продиктовать одноразовый код из СМС-сообщения. По легенде, этот код нужен для регистрации обращения в системе или для подтверждения корректировки. На деле же с помощью этого кода мошенники получают доступ к личному кабинету на Госуслугах или банковскому приложению – и могут вывести деньги или оформить кредиты. Также мошенники могут действовать через схему угрозы санкциями, пугают, что на долг уже начисляются пени, а в ближайшее время дело передадут приставам, которые арестуют счета. Чтобы остановить это предлагают срочно оплатить «штраф» по присланным реквизитам.

Запомните:

1. Не называйте коды из СМС никому. Сотрудники госорганов никогда не просят продиктовать одноразовые коды для доступа к вашим личным или банковским кабинетам.

2. Не переводите деньги по реквизитам, которые прислали по телефону или в мессенджере. Официальные уведомления от ФНС приходят в личный кабинет на сайте налоговой службы или на Госуслугах. Если есть сомнения – самостоятельно зайдите в свой кабинет и проверьте информацию.

3. Не поддавайтесь на запугивание. Если вам говорят, что прямо сейчас с вашим счетом или налогами что-то не так и нужно срочно что-то сделать – это тревожный знак.

4. Если у вас действительно есть налоговая задолженность, она не исчезнет от того, что вы переведете деньги по сомнительной ссылке. Правильным шагом будет разобраться в ситуации через официальные каналы.

ГСУ ГУ МВД России по Кемеровской области-Кузбассу