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.

Звонок сотрудника (Энергосбыт, Поликлиника, Пенсионный Фонд, Почта России, управляющая компания и т.д.)

Мошенники представляются сотрудниками Энергосбытовой компании, Поликлиники, Пенсионного Фонда, Почты России, управляющей компании и предлагают пересчитать электроэнергию или установить современный счетчик, новый домофон, сделать перерасчет пенсии, пройти любое медицинское обслуживание (диспансеризацию), получить посылку. Не важно, что говорят, важно, что спрашивают.

Как только жертву уговорили или обрадовали новым счетчиком, прибавкой к пенсии или чем-то еще, он даже 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. Перепроверяйте все, что говорят. Прервите разговор и перезвоните в организации, откуда поступил звонок и уточните информацию.

2. Никогда не передавайте содержимое из СМС-сообщения. Если передали информацию, то немедленно свяжитесь с поддержкой портала «Госуслуги» и заблокируйте учетную запись.

3. Сотрудники банков, правоохранительных органов, контролирующих организаций никогда не потребуют конфиденциальных данных из СМС-сообщений, не потребуют действий с вашими финансами, не отправят к банкомату, чтобы перевести деньги, не будут настаивать на сделках с недвижимостью.

Если просят хоть об одном из вышеуказанного – это мошенники.

Понятие «безопасный счет» - не существует.

Звонок (сообщение) от руководителя, коллеги, и в последующем ФСБ, банк и т.д.

Гражданину поступает звонок или сообщение от «руководителя» с предупреждением, что с ним свяжется сотрудник ФСБ. Для правдоподобности могут использовать, созданные нейросетями «дипфейки», копирующие голос или изображение, подменные телефонные номера или фальшивые документы. «Руководитель» будет указывать на большую важность задания, срочность, абсолютную секретность или большие риски для компании.

Дальше в дело вступит его сообщник, который будет запугивать и вынуждать оформить кредит, перевести наличными накопления или совершить противоправные действия.

Запомните:

1. Прежде всего не торопитесь и не паникуйте. Вывести из равновесия, это задача мошенника. Обратите внимание на адрес, номер телефона и аккаунт отправителя.

2. Если обычно начальник вам звонит по мобильной связи, а сейчас пишет в мессенджере, это повод насторожиться.

3. Не бойтесь позвонить начальнику и уточнить нюансы поступившей задачи. Вероятно, именно в этот момент окажется, что от имени начальника действуют мошенники.

4. Если вас пугают несанкционированными операциями по вашим счетам, иностранными переводами или другими действиями третьих лиц, которые могут вас скомпрометировать, позвоните в банк сам и выясните истинное положение.

5. Не выполняйте никаких действий под диктовку неизвестных, кем бы они не представлялись, не переводите средства, не оформляйте кредиты, не устанавливайте приложения на телефон.

Звонок сотрудника оператора сотовой связи

Мошенники представляются сотрудниками сотовых операторов и предлагают, и даже настаивают на продлении договора обслуживания номера. Для идентификации в системе могут попросить продиктовать паспортные данные и номер СНИЛС. Как только жертва диктует необходимые данные, следом поступает звонок от якобы сотрудника портала «Госуслуги», который сообщает о попытке взлома личного кабинета и для обеспечения защиты просит продиктовать код из СМС-сообщения.

Также, жертве может поступить сообщение в мессенджере или на электронную почту о том, что аккаунт на портале «Госуслуги» взломан и необходимо перезвонить на горячую линию по указанному номеру. Жертва перезванивает на тот номер, который указан в сообщении и диктует код из СМС-сообщения для блокировки аккаунта на портале «Госуслуги».

После передачи кода поступает звонок от якобы сотрудника банка или правоохранительных органов, начиная убеждать, что денежные средства на банковских счетах находятся под угрозой и для этого необходимо снять и перевести их на безопасный счет.

Если сбережений на банковских счетах нет, мошенники сообщат, что от имени жертвы поданы заявки на кредиты, необходимо подтвердить и также перечислить денежные средства на безопасный счет.

Мошенники пропадут, как только поймут, что жертва больше не сможет переводить денежные средства.

Запомните:

1. У SIM-карты нет срока действия. Договор услуги связи является бессрочным.

2. Не доверяйте звонкам, поступившим с неизвестных номеров. Всегда проверяйте информацию по телефону горячих линий, указанных на официальных сайтах организаций.

3. Не выполняйте инструкции незнакомцев, не сообщайте приходящие SMS-коды для подтверждения операций.

Покупка-продажа товаров на различных Интернет-сайтах (Авито, Дром, Юла, социальные сети: Вконтакте, Одноклассники и тд.)

Мошенники размещают объявление о продаже товара по заниженной цене. Когда жертва связывается с продавцом, тот сообщает, что находится в другом городе и предлагает оформить доставку. После чего, мошенник присылает фишинговую ссылку для оформления заказа, которая выглядит точно также, как и легитимный сервис. После ввода данных банковской карты мошенники отправляют ссылку на отслеживание посылки СДЭК по трек-номеру. Однако, трек-номер на официальном сайте СДЭК не отслеживается.

Также, есть ситуации, когда жертва размещает объявление на одном из Интернет-сайтов и на связь выходит мошенник, который изъявляет желание приобрести товар, но так как в данный момент находится не в городе, готов внести предоплату. Мошенник спрашивает номер банковской карты жертвы, чтобы перевести денежные средства, а после просит продиктовать СМС-код из сообщения, которое поступило из банка – якобы это необходимо для банковского перевода. Жертва в спешке называет СМС-код из сообщения, не успев понять, что это с его банковской карты происходит списание денежных средств.

Запомните:

1. Никогда никому не сообщайте коды из СМС-сообщения или CVV/CVC код карты.
2. Не переходите по ссылкам, не заполняйте ничего на сторонних сайтах.
3. Ориентируйтесь на среднюю для сервиса цену на интересующий вас товар. Мошенники занижают цены, чтобы повысить интерес.
4. Ознакомьтесь с отзывами реальных покупателей, прежде чем оформлять заказ.
5. 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.
6. Появились сомнения? Пишите в службу поддержки площадки.

Заработок на инвестициях или игры на бирже

Жертва откликается на рекламное объявление или предложение по телефону.

Мошенники могут представляться партнерами инвестиционной программы любого известного банка, пообещать баснословные проценты при минимальных вложениях. Жертву будут уверять, что никаких рисков, прибыль гарантирована, доход можно вывести в любой момент. Все, что потребуется – это заполнить анкету и скачать приложение. Создать личный кабинет поможет персональный менеджер. Дальше нужно только внести вложения. Первая же прибыль, которую видит жертва в личном кабинете, снимает остатки сомнений. Мошенники уверяют, что делать нужно крупные ставки, именно тогда доход будет огромным. Потерпевшие безоговорочно верят, берут большие кредиты и совершают переводы. Проблемы возникают, как только жертва пытается вывести прибыль. Тогда оказывается, что нужно пополнить личный счет на такую же сумму. Это ловушка! Мошенники специально создают такие условия, чтобы жертва вкладывала все больше и больше.

Запомните:

1. Прежде всего проявите бдительность и не верьте, что возможно получить большой доход за короткий срок. Ни одна официальная инвестиционная компания таких гарантий не даст.

2. Когда вы пополняете личный счет в банке, то делаете это в приложении банка или в банкомате. Здесь же преступники требуют совершать переводы по разным номерам телефона на имена физических лиц. Так поступают только мошенники.

Рассылка сообщений с текстом «Это ты на фото»?

Пользователям приходит сообщение от знакомых и не знакомых контактов в мессенджере с вопросом: «Это ты на фото»? и к письму прилагается закрытый файл в формате (ФОТО (9).apk).

При переходе по указанной ссылке вместо фотографии автоматически запускается установка вредоносной программы удаленного доступа.

После получения удаленного доступа злоумышленники заходят в банковское приложение и списывают все деньги и оформляют кредиты.

Запомните:

1. Не переходите по подозрительным ссылкам, присланным в том числе от знакомых;

2. В случае если вы уже прошли по ссылке необходимо незамедлительно включить телефон в режим полета, заблокировать банковские карты, отформатировать телефон до заводских настроек для удаления вирусного приложения.

Дополнительный заработок на маркетплейсах (ОЗОН, WB) – лайки, бронирование отелей, гостиниц

Жертве поступает сообщение о легком дополнительном заработке, предлагая забронировать номер в отеле, гостинице, с целью, повышения рейтинга, обещая вернуть стоимость бронирования и оплатить выполненную работу или же продвигать товары на «ОЗОН», «WB» и других маркетплейсах, получая денежные средства за каждый «лайк». Мошенник присылает ссылку, где жертва должна оставить отзыв или «лайк», и просят указать реквизиты банковской карты для перевода оплаты.

Запомните:

1. Отнеситесь внимательно к любым предложениям о трудоустройстве.
2. Не переходите по сомнительным ссылкам и пользуйтесь антивирусными решениями, которые предупреждают о сомнительном характере ресурсов.
3. Если вы ищете работу, лучше обратитесь на официальный сайт компании или специализированные ресурсы.

Взлом мессенджера – занять в долг знакомому

В социальной сети или мессенджере жертве поступает сообщение от знакомого из списка контактов. Он сообщает о том, что у него проблемы и срочно требуются денежные средства, просит выручить небольшой суммой. При этом, собеседник будет ссылаться на то, что некогда объяснять, для чего потребовались денежные средства, а вместо того, чтобы перевести по мобильному телефону, как правило привязанному к банковской карте, отправит новый номер банковской карты и пояснит, что ту заблокировали.

Запомните:

1. Прежде чем отправлять денежные средства, обязательно перезвоните и уточните просьбу. Убедитесь, что вы общались с реальными владельцами аккаунта.

2. После просьбы о денежном переводе не переходите по ссылкам в сообщениях.

3. Не переводите денежные средства на незнакомые карты, банковские счета, номера виртуальных кошельков, тем более, если они не привязаны к имени просящего.

4. Защитите свой аккаунт: подключите двухфакторную аутентификацию для доступа к нему, не сообщайте никому код авторизации.

5. Используйте уникальный пароль для каждого сервиса.

6. При малейшем подозрении на взлом аккаунта немедленно смените все пароли.

Родственник попал в беду

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками полиции за совершение преступления (совершил ДТП, хранил оружие или наркотики, нанес тяжкие телесные повреждения). Далее в разговор вступает «сотрудник полиции». Он уверенным тоном сообщает, что уже не раз «помогал» людям таким образом и для решения вопроса о не привлечении к ответственности необходимы денежные средства, которые в последствии жертва передает незнакомому человеку или переводит на банковский счет (абонентский номер телефона).

Запомните:

1. Незамедлительно прекратите разговор и свяжитесь со своим родственников и убедитесь в достоверности полученной информации.

2. Не нужно соглашаться на сомнительные сделки по передаче денежных средств.

3. Помните: дача взятки должностному лицу предусматривает уголовную ответственность.

Основные советы, чтобы не стать жертвой мошенников:

Не отвечайте на звонки с незнакомых номеров.

Прервите разговор, если он касается финансовых вопросов. Не торопитесь принимать решение.

Проверьте информацию в Интернете или обратитесь за помощью к близким родственникам.

Самостоятельно позвоните близкому человеку; в банк; в организацию и тд.

Не перезванивайте по незнакомым номерам.

Не сообщайте СМС-код из сообщения и номер СНИЛС.

Внимательно проверяйте от кого поступают сообщения.

Возьмите паузу и спросите совета у родных и друзей.

ГСУ ГУ МВД России по Кемеровской области-Кузбассу