Лекционный материал по профилактике мошенничеств и краж, совершенных с использованием информационно-телекоммуникационных технологий

За 11 месяцев 2024 года на территории Магаданской области зарегистрировано 523 хищения совершенных с использованием ИТТ, что на 8,9% ниже показателей прошлого года (574). В данное количество входят такие составы как кражи со счетов банковских карт (159), мошенничества (359) и вымогательство (5). Ущерб причинённый такими противоправными деяниями, составил более 217 млн. рублей. В 2023 году эта цифра была 245 млн. рублей.

В настоящее время на территории Магаданской области, как и на всей территории Российской Федерации, существует четыре самых основных способов совершения дистанционных преступлений:

1. Звонок от сотрудника банка или правоохранительных органов.
2. Взлом учетной записи в мессенджерах, с дальнейшей рассылкой контактам просьбы занять в долг денежные средства.
3. Дополнительный заработок (торги на бирже).
4. Покупка и продажа товаров в сети интернет.
5. Истечение срока действия сим-карты.
6. Взлом «Госуслуг».
7. Оформление кредитов в личных кабинетах кредитно-финансовых организаций, и покупка товаров на маркетплейсах, в связи с неотключением старого абонентского номера.

Звонок от имени сотрудника банка, следователя, прокуратуры, ФСБ и других ведомств и организаций. В разговоре звонящий предупреждает вас об экстренно возникшей ситуации (например, неизвестные лица пытаются оформить кредит, получили доступ к вашему личному кабинету банка и похищают деньги), настаивают на срочности и незамедлительности осуществления банковского перевода на «безопасные счета» просят назвать коды, полученные в смс-сообщениях. В результате граждане самостоятельно предоставляют доступ к банковским приложениям или переводят деньги на счета третьих лиц.

По данному способу хочу в очередной раз предупредить, напомнить, а может кого-то осведомить впервые – при поступлении звонков, где от вас требуются какие-то действия или сведения в части банковских реквизитов, кодов паролей из смс, перевода наличных денег на якобы безопасные счета-ячейки-кошельки – прекратите разговор, просто игнорируйте вызов с этого номера. Тем более сейчас в большинстве телефонов есть предустановленная функция по блокировке конкретного аб. номера. Таким образом, просто прекратив разговор, вы сохраните свои деньги и личное время, которое придётся тратить в случае факта хищения как минимум на поход в банк по восстановлению заблокированного личного кабинета, банковских карт.

Помните, что представители указанных ведомств и организаций никогда не звонят на телефон, тем более используя различные мессенджеры с

просьбой дистанционно без посещения конкретного ведомства выполнить какие-то действия и тем более сообщить какую-либо информацию по вашим банковским продуктам.

В последнее время, а точнее в первом квартале 2024 года, данный способ изменился и усовершенствовался, а именно изначально потенциальной жертве поступает звонок или сообщение в мессенджере телеграмм от неизвестного подписанного (раннее в данном мессенджере) как его руководитель, с полными его ФИО, в котором он сообщает, что вскоре поступит звонок от сотрудника правоохранительных органов, и необходимо выполнить все, что они потребуют. Далее вступает старая схема о безопасных счетах, подозрительных операциях и т.п.

Взлом учетной записи мессенджеров с дальнейшей рассылкой контактам просьбы занять в долг денежные средства.

Чтобы предостеречь себя от данного вида мошенничества,

Не нужно перезванивать на номер, откуда поступило сообщение через этот мессенджер, так как Вы вновь можете общаться со злоумышленником. Перезвоните используя обыкновенный аудио звонок и убедитесь лично в непосредственном контакте.

Почему произошел взлом аккаунта? Ранее скорее всего Вам поступило сообщение от знакомого (которого уже взломали) имеющегося в телефонной книге вашего устройства, о прохождении Вами по ссылке и осуществив голосование, но для этого предварительно зарегистрировавшись и дав доступ для стороннего устройства злоумышленника.

Про взлом ГОСУСЛУГ все просто. НЕ сообщайте никому ни под каким предлогом пароль от личного кабинета. Пароль нужно придумать сложнее, используя различные символы, заглавные буквы и т.д.

Дополнительный заработок. Торги на брокерских биржах. Тут всё просто – если не имеете определённого образования, навыков в данной деятельности, то поверьте – где бы вы не нашли объявление, или на вас вышел опытный брокер с заманчивым предложением, приумножить ваши деньги не получится. При этом если от вас никаких действий и участия (за исключением получения от вас денег) не требуется, то это 100% угроза и, как показывает практика, - потеря всех ваших накоплений и в большинстве случаев обременение кредитами, долгами.

Никогда настоящий трейдер или брокер не предоставит для перевода денег банковские счета и карты, счета абонентских номеров, электронных средств платежа и электронных кошельков ИМЕННО физических лиц. Для вывода денежных средств со счета у злоумышленника всегда имеются какие-проблемы, а именно: он просит Вас дополнительно внести деньги, для тех или иных услуг (страховка, налог, процент, округление суммы, отсутствие его руководителя для решения вопросов, проблемы в связи с политической обстановкой в мире и т.п.). Он может позволить вывести небольшие суммы, чтобы завоевать доверие и сподвигнуть Вас внести еще больше денег.

Инвестирование сейчас доступно во многих мобильных приложениях кредитных организаций. Рекомендуем проверить в интернете информацию о сайте, почитать отзывы. Но и здесь можно натолкнуться на фейк, так как мошенники создают сайты и пишут отзывы сами. Указанные на сайте абонентские номера, или те, с которых Вам поступит звонок, можно проверить в различных приложениях (как он записан в телефонной книге у других абонентов, например «Getcontact».

Покупка и продажа товаров на различных интернет сайтах.

Способ совершения преступления зависит от ситуации, в которую попадает потерпевший.

В случае, если гражданин выступает в качестве **покупателя** товаров и услуг в интернет-магазинах или на сайтах торговых площадок, он может попасть на недобросовестного продавца или заказать товар на так называемом фишинговом сайте: сайты-двойники являются распространенным видом интернет-мошенничеств.

В адресной строке сайта-двойника к названию популярного ресурса добавляется любая буква или символ, отличается домен.

Потребитель вводит данные карты на сайте-клоне, созданном мошенниками, и либо предоставляет данные своей банковской карты в руки мошенников, либо сразу осуществляет перевод денежных средств на их счета.

В полицию обращаются граждане, которые не убедившись в надежности интернет-магазинов и продавцов торговых интернет-площадок, переводили денежные средства в оплату одежды, запчастей, домашних животных, авиабилетов, бытовой техники, мотоциклов, снегоходов, автомобилей, а также аренды за квартиры, за оказание услуг по привороту и гаданию, трудоустройству, после чего расставались со своими деньгами.

Как проверить надежность продавца и сайта:

- Прочитать отзывы в интернете
- Посмотреть дату создания сайта (проверить можно например на интернет сайте www.trustorg.com «Доверие в сети»)
- При возможность исключить перевод аванса
- Проверить правильность написания адреса сайта
- Вас должно насторожить, если цена предложенного товара значительно ниже рыночной.
- Проверить профиль продавца на торговой интернет-площадке можно также по отзывам, дате создания профиля, истории продаж.

Если в качестве **продавца** выступает простой гражданин на разных интернет площадках, то:

- В телефонном разговоре злоумышленники путем введения в заблуждение получают у потерпевших данные карт, пароли к личному кабинету в онлайн-системах банка, якобы для перевода аванса или всей суммы сразу.

- Злоумышленники объясняют, что возникли трудности с переводом денег, произошла ошибка при вводе суммы, предлагают подойти к банкомату для получения аванса.

- Продавец также может отправить ссылку для оформления сделки через «сервис безопасных расчетов».

Как не стать жертвой мошенничества в данном случае:

- Обращайте внимание на абонентский номер, его регион (все преступления данной категории совершаются лицами, находящимися в других субъектах РФ);
- Не сообщайте реквизиты оборота б.к. и кода смс.

В случае, если вы продаете что-то дистанционно, покупатель может предложить вам пройти к ближайшему банкомату для получения аванса, либо всей суммы указанного в объявлении. Действуя под диктовку неизвестных на банкомате, сами того не подозревая, граждане осуществляют переводы на счета, указанные неизвестными.

При получении денежных средств за товар таким способом нет никакой необходимости идти к ближайшему банкомату, чтобы ни говорили мошенники (связано ли это с проблемой с картой и т.п.).

Истечение срока действия сим-карты.

При поступлении звонка от сотрудника того или иного оператора связи, который сообщил об окончании действия сим-карты, с просьбой продлить договор для продолжения ее функционирования, ЗНАЙТЕ срок действия сим-карт неограничен, и можно смело прервать телефонный звонок, так как это звонят мошенники.

Про взлом **ГОСУСЛУГ** все просто. НЕ сообщайте никому ни под каким предлогом пароль от личного кабинета. Пароль нужно придумать сложнее, используя различные символы, заглавные буквы и т.д.

Так же не стоит забывать, что при **смене абонентского номера**, который был подключен к услуге дистанционного банковского обслуживания, необходимо отключать эту услугу, в противном случае через определённое время старый номер поступит в пользование новому абоненту, которому не составит труда скачать мобильное приложение Банка, верифицироваться при помощи этого абонентского номера и войти в личный кабинет, где он сможет похитить денежные средства находящееся на счетах, оформить кредит и т.д. Также это относится к отвязке старого абонентского номера от известных маркетплейсов «Вайлдберриз» и «Озон».

Управление уголовного розыска