МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ - УРОКИ ЦИФРОВОЙ ГРАМОТНОСТИ

Методические материалы, предлагаемые УМВД России по Омской области.

За 12 месяцев 2024 года на территории Омской области зарегистрировано 5898 преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 1111 или 15,9% меньше, чем в 2023 году (АППГ - 7009).

Вместе с тем, ущерб, причиненный мошенниками жителям Омской области, увеличился на 140 млн рублей и превысил в 2024 году 1,69 млрд рублей (в 2023 году – 1,55 млрд). Ущерб, причиненный мошенниками потерпевшим на всей территории Российской Федерации, составил около 250 млрд рублей.

Основная доля преступлений совершена на территории областного центра – 4252 факта (72%). В районах Омской области зарегистрировано 1646 преступлений (28%).
От дистанционных преступлений в Омской области пострадали 5571 человек, из них 1637 (29,3%) – люди пожилого возраста. Чаще мошенничествам подвержены женщины: 3181 факт или 57%.

Основными способами завладения денежными средствами при совершении дистанционных преступлений, где ущерб является наиболее значительным, остаются:
Схема 1. Операторы сотовой связи.
Схема 2. Предложения от лжеброкеров, инвестирование на фондовых рынках.
Схема 3. Звонки или сообщения от знакомых с просьбами одолжить денег.
Схема 4. «Моя племянница участвует в конкурсе...» (переход по ссылкам).
Схема 5. Сообщение от «начальника».
Схема 6. Звонки и сообщения из банка.
Схема 7. Фишинг.
Схема 8. «Ваш родственник попал в ДТП».
Схема 9. Купля-продажа товаров в Интернете.

Схема 1. Операторы сотовой связи
Под видом специалистов известных телекоммуникационных компаний мошенники стараются получить доступ к аккаунту пользователя на портале «Госуслуги». Для этого они звонят жертве и утверждают, что действующий договор заканчивается и его необходимо продлить, иначе абонентский номер передадут другому клиенту. Идти никуда не нужно, все можно сделать по телефону, как уверяет злоумышленник: достаточно продиктовать код из СМС-сообщения.

В это время мошенник, владея информацией об абоненте (номер телефона, СНИЛС, ФИО), пытается зайти в его учетную запись на «Госуслугах», где указывает, что пароль от аккаунта утерян, и использует опцию направления пароля по номеру мобильного телефона абонента.
Следующий шаг – назвать мошеннику код. В сообщении, поступившем потерпевшему, указано, что эту информацию никому передавать нельзя и запрашивать её могут только мошенники. Однако собеседник настаивает, что именно он, как представитель оператора связи, отправил СМС для подтверждения личности абонента.
Таким образом, человек не продлевает договор, который на самом деле является бессрочным, а предоставляет данные для входа в личный кабинет на портале «Госуслуги» и всю информацию о себе, которая хранится на этом ресурсе.
Есть и другая цель, которую преследуют мошенники, представляясь оператором сотовой связи. Жертве также поступает звонок с предложением о смене тарифного плана, подключением опций, замены сим-карты. Алгоритм один – абоненту необходимо продиктовать код из СМС-сообщения, который придет на его номер. С помощью этого кода злоумышленник получает доступ к личному кабинету пользователя на официальном сайте оператора и настраивает переадресацию сообщений и звонков с номера жертвы на свой.
Это делается для того, чтобы в дальнейшем подтверждать разного рода операции: вывод средств с банковских карт абонента, оформление на него кредита.
В дальнейшем мошенники могут разыграть целый спектакль: позвонить и, представившись сотрудником правоохранительных органов, Центробанка или иных организаций, сообщить, что учетная запись гражданина на портале «Госуслуги» взломана, зафиксированы попытки перевода денег на Украину, оформления кредита, продажи недвижимости и т.п. Для пресечения этих действий необходимо выполнить ряд манипуляций. Как правило, в дальнейшем заходит речь о переводе денежных средств на некие «безопасные» счета.

ВАЖНО
Вы можете обновить персональные данные, обратившись за услугой лично – в офисе оператора сотовой связи или в личном кабинете на официальном портале (не по ссылке из СМС-сообщения).
Не называйте никаких данных незнакомым по телефону. Если сомневаетесь, позвоните оператору сотовой связи по номеру, который размещен на его официальном сайте.

Схема 2. Предложения от лжеброкеров, инвестирование на фондовых рынках.
Злоумышленники связываются с потенциальными инвесторами через социальные сети или звонят им под видом сотрудников известных

инвестиционных компаний. Предложение заманчивое – нужно лишь открыть брокерский счет и инвестировать от 10 000 рублей. Доход – не меньше миллиона.
Для открытия такого счета мошенники требуют установить приложение. Далее программа имитирует рост доходов от инвестиций, в том числе в криптовалюте. Как только у «инвестора» возникает желание вывести деньги со счета – начинаются проблемы. Лжеброкеры говорят, что сделать это сложно, но возможно: нужно пополнить счет еще раз, оплатить «страховку» или ежедневное размещение валюты в «европейской ячейке», либо найти поручителя, чтобы можно было обналичить средства. В итоге «инвестор» теряет свои деньги, а заодно и надежду на будущие миллионы.
Вариант этой мошеннической схемы – участие в уникальном инвестиционном онлайн-проекте известного банка. Завлекают потенциальных жертв при помощи писем на электронную почту. Злоумышленники, оформляя сообщение, копируют визуальный стиль финансовой организации: используют те же корпоративные цвета, логотип и другие элементы. Для участия в «выгодной» кампании предлагается перейти по ссылке из письма.
После жертве предложат пройти опрос: указать заработок, предпочитаемый способ хранения средств и контактные данные для связи с представителем организации, а также дадут доступ к специальному приложению. А уже там понадобится ввести данные своей банковской карты – с нее аферисты впоследствии и спишут деньги.

ВАЖНО
Проверьте сайт инвестиционной компании или брокера. Обратите внимание на реквизиты и наличие лицензии Банка России.
Откажитесь от услуг компании или ее представителей, если они просят перевести деньги за услуги на карту физического лица (либо через электронный кошелек).
Не верьте обещаниям гарантированного высокого дохода в короткие сроки, красивым картинкам, создающим иллюзию успеха брокера.

Схема 3. Звонки или сообщения от знакомых с просьбами одолжить денег.
Еще одна тактика злоумышленников – рассылка сообщений близким или друзьям с просьбой одолжить денег. Жертва, не убедившись в том, что общается с человеком, от имени которого приходят сообщения, спешит перевести деньги, уже потом узнает: страница собеседника взломана. Нередко в своих сценариях мошенники заходят и дальше – играют на чувствах потерпевших и сообщают, что требуются деньги, например, на лечение, операцию и т.д. Если раньше аферистам приходилось разыгрывать театральный спектакль, подделывая голос, то теперь за них это делает искусственный интеллект. Злоумышленники взламывают аккаунт пользователя, скачивают голосовые сообщения и на их основе генерируют нужный им монолог для дальнейшего обмана.

Схема 4. «Моя племянница участвует в конкурсе...»
Сценарий, схожий с сообщением от «знакомого», но тут мошенник сразу просит проголосовать за детей или племянников в детском конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, может скрываться вирус – он и откроет им доступ к вашему гаджету.
Данный способ является одним из самых распространённых по взлому аккаунтов в социальных сетях и мессенджерах: переходя по ссылке, пользователь попадает на фишинговый сайт. Чтобы проголосовать, его попросят авторизоваться. При вводе данных для входа в профиль их получат злоумышленники.

ВАЖНО
Не переходите по неизвестным ссылкам, даже если получили их от близких или знакомых. Договоритесь с родственниками о пароле или секретном вопросе, который нужно озвучить, если разговор кажется подозрительным. Такой шаг поможет распознать мошенника.

Схема 5. Сообщение от «начальника»
Злоумышленники пишут в мессенджерах пользователям под видом их действующих или бывших руководителей, политиков или лидеров общественного мнения. Для этого они создают реалистичные профили-двойники: используют фото человека из открытых интернет-источников, подписывают аккаунт нужной фамилией и именем. Аферист сообщает жертве о каких-то финансовых проблемах и о том, что с ним свяжется «сотрудник» правоохранительных органов, как правило федеральной службы безопасности. Причина может быть любой: от финансовых нарушений, выявленных в ходе проверки, до проведения секретной оперативной разработки, в которую якобы привлекут жертву для изобличения преступников.
Мошенник также может убеждать гражданина в том, что его деньги хотят украсть, перевести на счета СБУ или оформить на его имя кредит. Вариаций много, но выход один – вывести деньги на «безопасный счет». По легенде, это временная мера – на период поиска преступников. А потом всю сумму человеку якобы возместят наличными в приемной Банка России в Москве или другим удобным ему способом.

ВАЖНО
Помните, что к общению в сети, пусть даже с руководителем, нужно относиться максимально осторожно. При любом подозрительном вопросе необходимо связаться с ним лично либо по телефону, но никак не посредством мессенджера.

Схема 6. Звонки и сообщения из банка

В последнее время данная схема используется не на начальной стадии обмана: «представитель банка» подключается к уже «обработанной» его подельниками жертве. Наряду с предупреждениями об оформлении кредита на имя владельца банковской карты другим человеком или подозрительной операции по ней – появились и новые сценарии.

Мошенники под видом специалистов техподдержки финансовых организаций предлагают установить на смартфон приложение для поиска вирусов. На деле же это вредоносное программное обеспечение, которое дает доступ к телефону жертвы и его данным.

Еще один популярный сценарий – помощь в сохранении денежных средств. Аферисты под видом сотрудников Банка России сообщают жертве о том, что кто-то пытается похитить деньги с ее счета. Чтобы их спасти, надо перевести средства на «безопасный» счет. Обладая даже минимальными сведениями в отношении потенциальной жертвы, злоумышленники используют уже известные сценарии: представляются сотрудниками ФСБ, МВД, Центробанка, Росфинмониторинга, портала «Госуслуг», Пенсионного фонда и т.п. Для убедительности они могут присылать фотографии фейковых служебных удостоверений и документов (постановления, договоры, счета, содержащие персональные данные потерпевшего) и даже общаться с жертвой посредством видеосвязи, имитируя обстановку служебного кабинета.

ВАЖНО

Пользуйтесь только официальными ресурсами финансовых организаций. Если вам звонят сотрудники банка, и разговор с ними кажется подозрительным, перезвоните на официальный номер, размещенный на сайте финансовой организации или на оборотной стороне банковской карты. Там же вы можете найти ссылки на официальные банковские приложения и скачать их.

Никакие ведомства не наделены полномочиями по решению вопросов финансовой безопасности дистанционно. По любым проблемным ситуациям заявитель должен обращаться лично в отделение банка либо в полицию.

Схема 7. Фишинг

Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям (англ. «fishing» – рыбная ловля, выуживание). Мошенники создают точные копии официальных сайтов торговых и других организаций, предлагают ввести персональные данные, информацию о банковской карте и получают полный доступ к деньгам граждан.

Необходимо обращать внимание на адресную строку сайта. Домен фишингового ресурса может иметь отличие от домена оригинального сайта всего в одну букву.

В результате успешного фишинга злоумышленники могут получить логин и пароль пользователя, его персональные данные – фамилия, имя, отчество,

номер телефона, адрес электронной почты, а также платежную информацию (номер банковской карты, срок действия, CVC/CVV-код, владелец, код подтверждения операции).

ВАЖНО

Никогда не предоставляйте личные и банковские данные третьим лицам. Банки, сервисы и магазины никогда не присылают неожиданных писем с просьбой перейти по ссылке, изменить пароль, ввести номер банковской карты и секретный код подтверждения или сообщить личные данные.

Никогда не оставляйте номер телефона на подозрительных сайтах и не отправляйте СМС на короткие номера. Мошенники создают сайты, на которых вы якобы можете бесплатно посмотреть или скачать приглянувшийся фильм, но сначала надо оставить телефон или отправить сообщение на короткий номер. Так с вашего счета могут списать внушительную сумму за СМС, а сам телефон попадет в базу спамеров.

Обращайте внимание на короткие URL. Сокращенные URL-адреса выглядят короткими и симпатичными, начинаясь, например, с bit.ly (популярный сервис для сокращения ссылок), но злоумышленники используют их для скрытия подозрительных сайтов, распространяя подобные ссылки в социальных сетях и мотивируя перейти по ним.

Такие сокращенные URL-адреса могут маскироваться под официальные сайты. Прежде чем переходить по ним, проверьте эти адреса с помощью сервисов вроде CheckShortURL на наличие вредоносных программ.

Схема 8. «Ваш родственник попал в ДТП»

Людям пенсионного возраста звонят с неизвестного номера. Звонок может поступить как на стационарный, так и на мобильный телефон. Звонящий представляется сыном, дочерью, другим близким человеком. Он сообщает, что его задержала полиция. Чаще всего речь идёт о ДТП: нарушил правила дорожного движения, и по его вине пострадали люди. Изменения в голосе мошенник объясняет тем, что в аварии он повредил лицо и ему трудно говорить.

Затем к разговору подключается «полицейский», который говорит, что готов помочь, но для этого надо передать ему определённую сумму денег. Если вы откажетесь это сделать, вашего родственника ждёт тюрьма. Передать деньги надо немедленно, потому что потом будет поздно.

К пенсионерам пребывает курьер, который забирает деньги и переводит их мошенникам, оставляя себе оговоренный процент.

ВАЖНО

Объясните пожилым родственникам: прежде чем выполнять любые указания, полученные по телефону, нужно взять паузу, сообщить о случившемся близким людям и обсудить с ними сложившуюся ситуацию.

В случае звонка от имени родственника или знакомого алгоритм действий должен быть один: прервать разговор и позвонить этому человеку. Скорее всего, он возьмет трубку и сообщит, что с ним все хорошо. Даже если он не подходит к телефону – это ещё не повод немедленно переводить деньги. Подождите, пока он перезвонит, или разыщите его через общих знакомых.

Схема 9. Купля-продажа товаров в Интернете

Мошенники наряду с добропорядочными гражданами активно используют сайты бесплатных объявлений. На них очень удобно продавать и покупать товары или искать работу.

Люди, которые часто размещают объявления на сайте, как правило, подробно заполняют свой профиль. У них есть рейтинг и отзывы тех, кто пользовался их услугами. На многих сайтах существует возможность подтверждения профиля, и постоянные пользователи ею не пренебрегают. Однако мошенники могут разместить чужую фотографию, подтвердить профиль с помощью чужого паспорта и накрутить себе рейтинг. Невозможно подделать только дату регистрации профиля.

Реальный продавец заинтересован в том, чтобы дать как можно более подробную информацию о товаре: это привлечёт внимание и поможет избежать дополнительных вопросов со стороны потенциальных покупателей. Если описание товара слишком общее, в нём нет фотографий или они взяты из интернета, это должно насторожить.

Если вас заинтересовал товар, изучите профиль продавца, почитайте отзывы. Свяжитесь с ним, попросите прислать фотографии товара с разных ракурсов, лучше видеозапись, задайте все интересующие вас вопросы. Если продавец отказывается присылать фото, не отвечает на ваши вопросы – лучше поискать товар в другом месте.

Если продавец торопит с покупкой, настаивает на предоплате до отправки заказа, просит оплатить услуги курьера или службы доставки переводом на карту, а не через сервис объявлений, переносит общение в мессенджер – скорее всего, это мошенник.

Обман может иметь место и со стороны «покупателя», который запрашивает данные банковской карты якобы для внесения предоплаты, а в итоге похищает ваши сбережения.

Будьте бдительны! Прежде чем совершать сделки купли-продажи, убедитесь в надежности собеседника. Если хоть немного сомневаетесь – лучше откажитесь от сделки. Так вы убережете себя от ненужных переживаний и трат.

УМВД России по Омской области

Адрес полной версии этой страницы: https://digital.omskportal.ru/oiv/digital/etc/metod