УПРАВЛЕНИЕ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО АСТРАХАНСКОЙ ОБЛАСТИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

По вопросам профилактики преступлений, совершаемых с использованием информационно-коммуникационных технологий и мерам противодействия им

Астрахань - 2025

Киберпреступники и мошенники не имеют какой-либо наиболее распространённой схемы, которую бы они использовали для проведения атак на жителей Астраханской области. Злоумышленники легко адаптируются под кризисные ситуации, стараясь нажиться на эмоциональном состоянии людей. При этом, выбор способа мошенничества, прежде всего, зависит от целей, которые ставят перед собой аферисты, от наличия у них соответствующих ресурсов, времени на подготовку и квалификации.

ОБК УМВД России по Астраханской области выделены несколько наиболее распространенных способов совершения преступлений:

- Схема 1. Звонки и сообщения из банка.
- Схема 2. Звонки и сообщения от государственных ведомств.
- Схема 3. Операторы сотовой связи.
- Схема 4. Предложения от лжеброкеров и инвестиционных компаний.
- Схема 5. Общение с работодателем.
- Схема 6. Звонки или сообщения от знакомых.
- Схема 7. Сайты бесплатных объявлений.

Социальные сети и мессенджеры чаще всего используются для максимального охвата потенциальных жертв. При этом там обычно мошеннические схемы достаточно примитивные, поэтому их нельзя назвать эффективными.

Наиболее выгодным способом мошенничества для аферистов являются обычные телефонные звонки, которые приносят киберпреступникам достаточно неплохие доходы, потому что многие применяемые в ходе них схемы давно отработаны, злоумышленники, давно присутствующие в этой сфере деятельности, имеют достаточно высокие навыки применения методик социальной инженерии.

В случае проведения крупных единовременных кибератак максимально прибыльными для злоумышленников сейчас являются рассылки с вложениями в виде вредоносного ПО (чаще всего это программы-вымогатели). Если пользователь откроет такое письмо, скачает и запустит на своём устройстве вложенный файл, то все его данные на компьютере будут зашифрованы. Подобные действия особенно опасны в случае, если открытие файла происходит на корпоративном устройстве. В этом случае злоумышленники могут скомпрометировать всю IT-инфраструктуру организации.

Схема 1. Звонки и сообщения из банка

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 в ЦБ РФ. По легенде это временная мера – на период поиска преступников. А потом всю сумму человеку якобы возместят наличными в приемной Банка России в Москве.

Наряду с лживыми угрозами 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. Это вредоносное программное обеспечение, которое дает доступ к телефону жертвы и его данным.

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. Там же вы можете найти ссылки на официальные банковские приложения и скачать их.

Схема 2. Звонки и сообщения от государственных ведомств

Часто мошенники звонят или пишут человеку якобы от лица сотрудников ФСБ, Росфинмониторинга, ФНС, Социального фонда России, портала «Госуслуги». Самая распространенная уловка – предложение получить какую-либо государственную выплату. Схема классическая: вы нам данные карты, мы вам – деньги. Есть и другой сценарий. Например, звонок от представителей следственных органов или Росфинмониторинга с угрозой блокировки счета, по которому якобы зафиксированы сомнительные операции. Чтобы этого избежать, мошенники требуют оплатить штраф. Для убедительности они могут даже прислать квитанцию на официальном бланке ведомства.

Если вы получили подобные сообщения – проигнорируйте их и обратитесь напрямую в государственную организацию.

Схема 3. Операторы сотовой связи

Под видом специалистов известных телекоммуникационных компаний мошенники стараются получить доступ к аккаунту пользователя «Госуслуги».

Они звонят жертве и утверждают, что действующий договор заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. Идти никуда не нужно, все можно сделать по телефону, уверяет злоумышленник. Достаточно продиктовать код из смс. Следующий шаг – перейти по ссылке, где нужно ввести еще один код.

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 связи. Жертве также поступает звонок с предложением по смене

тарифного плана, подключением опций, замены sim-карты. Чтобы реализовать любое из действий, абоненту необходимо продиктовать код из смс, который придет на его номер. С помощью этого кода злоумышленник получает доступ к личному кабинету пользователя на официальном сайте оператора. А уже там он 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.

Вы можете обновить персональные данные, обратившись за услугой лично – в офисе оператора связи или в личном кабинете на его официальном портале (но не по ссылке из смс).

Не называйте никаких данных незнакомым по телефону. Если сомневаетесь, позвоните оператору связи по номеру, который размещен на его официальном сайте.

Схема 4. Предложения от лжеброкеров и инвестиционных компаний

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 якобы рост доходов от инвестиций, в том числе в криптовалюту. Как только у «инвестора» возникает желание вывести деньги со счета – начинаются проблемы. Лжеброкеры говорят, что сделать это сложно. Нужно пополнить счет еще раз на определенную сумму, 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.

Один из вариантов 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 и далее для убедительности 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 потом и спишут деньги.

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). Обязательно заключите договор и запрашивайте отчет об оказании брокерских услуг.

Не верьте обещаниям гарантированного высокого дохода в короткие сроки.

Схема 5. Общение с работодателем

Под видом будущего работодателя мошенники проводят собеседование, где они просят кандидата заполнить анкету. Один из ее пунктов – номер карты и другие ее данные. На нее злоумышленники обещают производить оплату. Чтобы ничего не пропустить, они включают запись экрана. Некоторые мошенники просят указать информацию по нескольким банковским картам, если какую-то якобы не примет бухгалтерия.

Вместо пополнений с банковской карты соискателя в будущем происходят списания, а на работу его так и не устраивают. Находясь в поиске работы, можно не только потерять деньги, но и нарушить закон, став соучастником преступных действий.

В последнее время также участились случаи вовлечения граждан в преступную схему, за небольшое денежное вознаграждение, связанное с оформлением банковских карт, а также сим-карт.

Дропперы или дропы (от английского drop — бросать, капать) – подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт.

Часто жертва не осознает, что вовлечена в преступную схему. Ведь объявление о работе, на которую она устраивается, не выглядит подозрительно. А будущий работодатель после собеседования предоставляет договор, оговаривает условия труда, сроки выполнения работы и другие нюансы.

Внимательно изучайте предложение от будущего работодателя и отзывы о нем. Не верьте обещаниям легкого заработка с минимальной затратой собственного времени.

При общении сохраняйте холодную голову, не поддавайтесь эмоциям, а главное – следите за данными, доступ к которым предлагается предоставить.

Схема 6. Звонки или сообщения от знакомых

Еще одна тактика злоумышленников – рассылка сообщений с просьбой одолжить денег близким или друзьям. Порой в своих сценариях мошенники

заходят и дальше – играют на чувствах жертвы и сообщают, что ее родственник попал в беду. 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 монолог для дальнейшего обмана.

Мошенники взламывают страницы в социальных сетях и обманом выманивают деньги у граждан. Практически каждый современный пользователь Интернета имеет личную страничку в одной, а то и нескольких социальных сетях, где можно переписываться с друзьями, делиться фотографиями и иной информацией. Однако от граждан, пользователей той или иной социальной сети, все чаще стали поступать заявления в полицию о мошеннических действиях неизвестных лиц, которые посредством социальных сетей от имени их знакомых обманным путем завладевают денежными средствами.

Как правило, мошенники досконально изучают взломанную страницу пользователя и пишут от его имени самым близким людям, доверие которых высоко.

Чтобы обезопасить себя от взлома аккаунта, ОБК УМВД России по Астраханской области рекомендует придерживаться следующих правил:

- создавайте сложные пароли, используя цифры, символы, а также прописные и заглавные буквы;

- никогда не переходите по подозрительным ссылкам, особенно если их прислали незнакомые люди;

- при входе на свою страницу, где необходимо ввести данные, всегда смотрите на адрес сайта в поисковой строке браузера, он может отличаться от оригинального знаком или одной буквой и оказаться фальшивым.

Схема 7. Сайты бесплатных объявлений.

Как безопасно пользоваться сайтами объявлений. С помощью сайтов объявлений очень удобно продавать или покупать товары или искать новую работу. Об этом знаете не только вы, но и мошенники, которые пытаются заработать на вашей доверчивости. Разбираемся, как не попасться на их уловки.

На что надо обращать внимание и что делать, чтобы вычислить мошенников? Прочитайте объявление. Обратите внимание на следующие моменты: профиль продавца, описание товара, стоимость товара, необходимость внесения предоплаты до отправки товара.

Если продавец под любым предлогом просит внести предоплату до отправки заказа, оплатить услуги курьера или службы доставки переводом на карту, а не через сервис объявлений, то скорее всего это мошенник. Он будет выдумывать различные предлоги, чтобы выманить деньги. Никогда

не вносите предоплату, если это не предусмотрено сервисом объявлений — только он может гарантировать безопасность сделки. Не переводите деньги на карту продавца – таким образом вы просто дарите их её владельцу. Если он окажется мошенником, то вернуть ваши средства не удастся.

Неправомерный доступ к Единому порталу Государственных и муниципальных услуг.

Участились случае когда мошенники стали рассылать push-уведомления о необходимости верифицировать номер телефона, подтвердив паспортные данные. Ссылка в сообщении ведет на фейковый сайт мобильных операторов, на котором предлагается заполнить анкету: номер телефона, ФИО и дату рождения.

После заполнения сайт переводит на фейковую страницу входа на портал «Госуслуги», где пользователь должен ввести логин и пароль к личному кабинету. Так мошенники получают и данные доступа к «Госуслугам», и подтвержденную информацию об абоненте.

Зачем мошенники хотят зайти в Госуслуги? Что они там смогут сделать? Одна из распространенных схем мошенников направлена на то, чтобы получить доступ к личному кабинету жертвы на Госуслугах. Что злоумышленники могут сделать, если получат логин и пароль от Госуслуг?

Запросить кредитную историю. Самое меньшее, что могут сделать злоумышленники — получить конфиденциальную информацию о человеке. В нее входит кредитная история, размер счета в банке, размер долга (если он есть), а также другая финансовая информация. В дальнейшем мошенники могут использовать эти данные в других схемах, например, при попытке сообщить о краже денег жертвы от лица сотрудника банка, полиции или МВД.

Получить доступ к электронной подписи. Все чаще различные операции с документами можно проводить без личного присутствия. Для этого достаточно иметь нужные бумаги и электронную подпись. Получив доступ
к ней, мошенники смогут подделать документы и выполнить целый ряд действий, которые обернутся для жертвы серьезными проблемами.

Если электронная подпись попадет в руки мошенников, они смогут:

1. Переоформить или продать недвижимость жертвы. Оформить на ее имя кредит.

2. Сдать поддельную отчётность в налоговую, чтобы получить возмещение.

3. Зарегистрировать сомнительное юридическое лицо на имя жертвы.

На этом список возможностей электронной подписи не заканчивается, однако этими операциями мошенники захотят воспользоваться с большей вероятностью.

Получить доступ к личной информации о человеке. Портал Госуслуги также выступает своеобразным хранилищем для различных документов пользователей, к которым не должны иметь доступ посторонние. Так, на Госуслугах хранятся полные данные ФИО, номер телефона, паспортные данные, адрес регистрации, СНИЛС, ИНН, данные водительского удостоверения и другие документы. Злоумышленники смогут использовать это в любых целях, так как многих из этих документов уже достаточно для подтверждения личности и совершения финансовых операций.

С этими данными злоумышленники смогут:

1. Зарегистрировать электронные кошельки для проведения мошеннических операций.

2. Оформить кредит или микрозайм.

3. Оформить онлайн-заявление о переводе средств человека в любой негосударственный пенсионный фонд, чтобы получить возмещение.

4. Манипулировать личной информацией о человеке в других мошеннических схемах.

Оформить eSIM с помощью Госуслуг. Еще один скорее неприятный, чем опасный вариант — мошенники оформят на имя пользователя eSIM через портал Госуслуг. Эта услуга поддерживаются несколькими операторами связи и провести операцию можно дистанционно без личного посещения салона связи. И хотя сам факт оформления мошенниками eSIM может не вызывать особых опасений, известны случаи, когда злоумышленники после оформления SIM-карты привязывали новый номер к банковскому профилю жертвы в том числе из-за халатности банковских работников. Также проблемой может стать массовое оформление eSIM-карт на имя жертвы, которые в дальнейшем будут использоваться неизвестными для других мошеннических схем.

Как противостоять воздействию телефонных мошенников?

Теперь, когда вы знаете, какие приёмы воздействия используют мошенники, вам будет проще им противостоять, запомните самое главное:

- Прежде чем выполнять любые указания, полученные по телефону, возьмите паузу, сделайте три глубоких вдоха-выдоха, позвоните близким людям и обсудите с ними сложившуюся ситуацию.

- Если вам звонят от имени вашего родственника или знакомого и просят перевести деньги свяжитесь с ним лично. Даже если он не подходит к телефону — это ещё не повод немедленно переводить деньги. Подождите, пока он перезвонит, или разыщите его через общих знакомых.

- Данные о ваших банковских счетах, номер карты, пин-код или CVV/CVC/CVP- код, код из СМС и любые другие сведения для совершения банковского перевода нельзя сообщать никому.

- Вы никогда не можете быть уверены в том, что позвонивший вам человек — именно тот, кем представляется. Если вам поступил

подозрительный звонок, положите трубку и перезвоните сами в организацию, от имени которой к вам обратились.

- Ни банки, ни полиция, ни другие организации не решают вопросы по телефону, особенно в срочном порядке. Даже если вам угрожают уголовной ответственностью за отказ сотрудничать — знайте, что телефонные угрозы не имеют юридической силы. Если вам поступил подозрительный звонок, положите трубку и перезвоните сами в организацию, от имени которой к вам обратились.

Какие фразы произносят только мошенники?

К счастью, мошенники работают по скриптам, в которых четко прописано, какие фразы они должны произносить. По этим фразам вы можете их определить.

Вот основные:

1. Давайте уточним ваши данные: назовите номер своего паспорта, номер банковской карты.

2. Сколько у вас счетов в нашем банке?

3. Уточните баланс каждого вашего счёта.

4. В каких ещё банках у вас есть счета?

5. Нам надо составить заявку по факту мошеннических действий. Какую заявку будем составлять: обычную или экстренную?

Напоминаем:

1. Настоящий сотрудник банка видит в информационной системе все данные клиента, информацию о его счетах и количестве денег, которые на них находятся.

2. Банки работают автономно, сотрудник одного банка никак не может повлиять на то, что происходит в другом банке.

3. Если банк заподозрил, что с вашим счётом совершаются мошеннические действия, он заблокирует счёт без всякой заявки.

Как не попасться на уловки аферистов.

Российские пользователи в последние годы достаточно часто попадаются на уловки киберпреступников и телефонных мошенников, использующих не только методики социальной инженерии, но и приёмы гипноза, чтобы заполучить деньги с потенциальной жертвы.

Аферисты могут использовать всевозможные выдуманные легенды для предлога перевода денежных средств, представляясь при этом сотрудниками неких серьёзных госструктур.

Напоминаем, сотрудники полиции никогда не будут:

- звонить гражданам и заявлять, что тем необходимо принять участие в некой операции по задержанию мошенников или иных преступников;

- требовать или просить граждан выполнить перевод денежных средств на какие-либо резервные счета, оформить кредит и совершить иные банковские операции.

Кроме того, Центральный Банк России не занимается сотрудничеством с физическими лицами, не открывает им какие-либо расчётные и банковские счета, не имеет никаких «специальных» или «безопасных» счетов.

Если кто-то по телефону или в сети Интернет просит выполнить перевод денежных средств на подобные счета, то необходимо срочно прекращать общение с таким человеком, поскольку со 100% вероятностью это мошенник.

Злоумышленники активно рассылают по электронной почте, в социальных сетях и мессенджерах сообщения российским пользователям с предложением о получении пострадавшим от проведения военной спецоперации всевозможных компенсаций от государства.

При этом злоумышленники в рамках реализации таких мошеннических схем могут представляться сотрудниками различных благотворительных фондов, правоохранительных органов и государственных структур.

В своих сообщениях аферисты просят заинтересованных граждан связаться с ними через личные сообщения в социальной сети или в мессенджере, чтобы можно было заполнить анкеты «от первого лица».

Настоятельно не рекомендуем верить в подобные сообщения, направленные исключительно на выведывание конфиденциальной информации либо склонение к переводу под различными предлогами денежных средств.

Обращаем внимание, что информация обо всех возможных компенсациях представлена в открытом доступе на официальных ресурсах и страницах социальных сетей профильных государственных учреждений, в том числе и региональных ведомств.

Как защититься от различных киберпреступных и фишинговых сайтов.

Что сегодня крайне актуально в условиях широкого распространения различных мошеннических схем, направленных на принуждение российских граждан к скачиванию сомнительного программного обеспечения и вирусов.

Для обеспечения высокого уровня защиты от фишинговых ресурсов необходимо, прежде всего, обратить внимание на адрес сайта и его содержание.

К основным признакам, с помощью которых можно точно установить факт нахождения на откровенно мошенническом ресурсе, относятся:

- неправильно написанные (дополнительные символы, цифры и т.п.), подозрительные или непонятные URL-адреса;

- отсутствие SSL-сертификата у ресурса; наличие ошибок в грамматике, орфографии, дизайне при оформлении и наполнении сайта;

- ссылки на скачивание какого-либо файла, интересующего пользователя, со стороннего ресурса.

Настоятельно не рекомендуется переходить по коротким ссылкам с популярных сервисов, таких как bit.ly или goo.gl, даже в том случае, если они приходят от близких и знакомых, поскольку аккаунты последних могут быть скомпрометированы.

Если вредоносное программное обеспечение скачано на телефон или компьютер, ничего страшного в этом нет.

Основная проблема будет заключаться в том, если этот файл будет открыт на устройстве. В данном случае необходимо как можно быстрее отключить устройство от интернета.

В ситуации, если файл ещё не запущен, то необходимо проверить его с помощью специализированных сайтов для анализа файлов и ссылок.

УМВД России по Астраханской области