приложение № 1

Памятка
о видах и способах совершения преступлений с использованием информационно-коммуникационных технологий и меры противодействия им.

Киберпреступники и мошенники не имеют какой-либо наиболее распространённой схемы, которую бы они использовали для проведения атак на российских пользователей.

Они 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.

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.

Проведенным анализом возбужденных на территории Саратовской области уголовных дел по преступлениям, связанных с использованием информационно-коммуникационных технологий, а также зарегистрированных в КУСП материалов по

сообщениям о преступлениях данной категории, можно выделить несколько наиболее распространенных способов совершения деяний рассматриваемой категории:

Схема 1. Операторы сотовой связи.
Схема 2. Предложения от лжеброкеров.
Схема 3. Общение с работодателем.
Схема 4. Звонки или сообщения от знакомых.
Схема 5. Оплата услуг по фейковому QR-коду.
Схема 6. Звонки и сообщения из банка.
Схема 7. Звонки и сообщения от государственных ведомств.

Схема 1. 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.

ВНИМАНИЕ!!!
Договоры, заключаемые абонентом с сотовыми операторами, не предусматривают ограниченного срока пользования номером.

Будьте бдительны и предупредите своих близких!

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.

ВАЖНО

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 2. Предложения от лжеброкеров

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.

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 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.

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).

Обязательно заключите договор и запрашивайте отчет об оказании брокерских услуг.

Не ведитесь на обещания гарантированного высокого дохода в короткие сроки.

Схема 3. Общение с работодателем

Собеседование с будущим работодателем – волнительная процедура. Порой мошенники пользуются растерянностью соискателей и крадут личные данные прямо во время онлайн-встречи.

Под видом будущего работодателя мошенники проводят собеседование, где они просят кандидата заполнить анкету прямо во время зума. 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 дроппером.

В последнее время именно этот мошеннический сценарий становится популярным, а его жертвами становятся студенты и пенсионеры.

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.

ВАЖНО

Внимательно изучайте предложение от будущего работодателя и отзывы о нем.

Не ведитесь на обещания 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 4. 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.

Существует и другой сценарий – просьба проголосовать за детей или племянников в детском конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который откроет им доступ к вашему гаджету.

ВАЖНО

Не переходите по неизвестным ссылкам, даже если получили их от близких или знакомых.

Договоритесь с родственниками о пароле или секретном вопросе, который нужно назвать, если разговор кажется подозрительным. Такой шаг поможет раскусить намерения мошенника.

Схема 5. Оплата услуг по фейковому QR-коду

Сегодня, чтобы получить какую-либо услугу или оплатить товар, достаточно навести камеру на QR-код. Например, им можно воспользоваться, чтобы взять в аренду самокат или портативное зарядное устройство для гаджета. Правда, вместо прогулки с ветерком и заряженного аккумулятора телефона можно получить пустой банковский счет.

Дело в том, что такой QR-код ведет не на официальный сайт сервиса, а на поддельный ресурс, через который аферисты крадут деньги и данные карты.

ВАЖНО

Оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета.

Схема 6. Звонки и сообщения из банка

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.

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.

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.

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

Схема 7. 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.

ВАЖНО

Помните, что подобные ведомства не наделены полномочиями по аресту денежных средств, не оказывают платных услуг по оформлению документов, а также не рассылают подобные письма и не звонят по телефону или в мессенджерах.

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

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.

Люди, которые часто дают 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. Серьёзные сервисы объявлений стараются бороться с мошенниками и блокировать их, поэтому такие профили существуют недолго. Конечно, не каждый недавно зарегистрировавшийся человек, не имеющий рейтинга, — мошенник. Однако к обладателям таких профилей надо относиться с особым вниманием.

Описание товара.

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.

Стоимость товара.

Как правило, выставляя товар на продажу, люди оценивают его на основании аналогичных объявлений. Конечно, бывают случаи, когда реальный товар продается очень дёшево. Тем не менее, если вы видите объявление, где стоимость товара значительно ниже, чем у аналогов, будьте особенно внимательны.

Что делать?

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

Настойчивость продавца

Вы связались с продавцом, а он говорит, что желающих приобрести товар очень много, торопит с покупкой. Также он настаивает на том, чтобы вы внесли предоплату не через сервис объявлений, а переводом на его карту. Будьте осторожны, такой приём часто используют мошенники. Их цель — не дать вам всё хорошенько обдумать.

Что делать?

Не торопитесь с покупкой. Вносите оплату только через сервис объявлений.

Предоплата 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 у вас деньги.

Что делать?

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.

Перенос взаимодействия в мессенджер

На сайтах объявлений существуют чаты для общения продавцов и покупателей. Как правило, в них встроены инструменты распознавания мошеннических фраз. Они блокируют ссылки на сторонние ресурсы, предупреждают о риске, если собеседники публикуют номер телефона. Поскольку чаты затрудняют деятельность мошенников – они стараются перевести диалог в сторонний мессенджер, где нет никаких ограничений.

Что делать?

Скройте свой номер телефона в настройках профиля. Там же включите функцию запрета звонков, чтобы мошенники не застали вас врасплох. Общайтесь только в чате на сайте объявлений. Ни под каким предлогом не переходите в обычный мессенджер.

Присылают ссылку для оплаты или просмотра информации

Если вы всё-таки начали общаться с продавцом в стороннем мессенджере, вам могут прислать ссылку якобы для просмотра более подробной информации о товаре или для оплаты.

Мошенники взламывают страницы в соцсетях 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, УБК МВД России 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.

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.

Многие пользователи столкнулись с новой схемой «угона» учетных записей (аккаунтов) в мессенджерах Telegram и WhatsApp.

Кто-то из контакт-листа просит принять участие в некоем онлайн-голосовании и присылает ссылку на сайт. Для учета голосов требуется ввести свой номер телефона и код верификации.

Чтобы не лишиться своей учетной записи не поленитесь, перезвоните тому абоненту, от которого пришло сообщение и уточните, он ли его отправил.

То же самое нужно сделать когда кто-то под благовидным предлогом просит перевести ему деньги.

Не дайте обмануть себя и ваших близких!

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 чётко 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.

Разбёрем самые популярные сценарии мошенников и попробуем на примерах понять, какие манипулятивные техники они используют.

Родственник в беде

Вам звонят с неизвестного номера. Звонивший представляется вашим сыном, дочерью, другим близким человеком. Он сообщает, что его задержала полиция. Чаще всего речь идёт о ДТП или драке. Затем к разговору подключается якобы полицейский, который говорит, что готов помочь, но для этого надо передать ему определённую сумму денег. Если вы откажетесь это сделать, вашего родственника или знакомого ждёт тюрьма (Страх потери или преследования). Передать деньги надо немедленно, потому что потом будет поздно (Не дать времени подумать).

Еще один вариант сценария «родственник в беде»

Вы получаете СМС или сообщение в мессенджере с просьбой перевести деньги по номеру телефона. То, что номер вам не знаком, злоумышленники объясняют тем, что ваш сын или дочь попали в беду, потеряли свой телефон и теперь очень ждут вашей помощи (страх потери).

Звонок из службы безопасности, полиции, ФСБ, Центрального банка, государственных структур

Вам звонят с неизвестного номера, обращаются по имени и отчеству (доверительныеи отношения), представляются сотрудником службы безопасности банка, главным специалистом Центрального банка (звонок от значимого лица) и говорят, что с вашей карты пытались снять деньги (страх потери). Чтобы этого не произошло, надо немедленно подтвердить данные своей банковской карты и сообщить код из СМС (не дать времени подумать). Если вы не сделаете это прямо сейчас, деньги спишутся (запугивание).

Ещё один сценарий — мошенники представляются сотрудниками полиции или ФСБ (звонок от значимого лица)

Мошенники говорят, что на ваше имя оформлен кредит, ваши деньги пытаются украсть либо вы должны принять участие в расследовании преступления (страх потери или преследования). Чтобы спасти свои деньги или помочь в расследовании, надо немедленно перевести их на безопасный счёт, который они вам назовут. Поскольку операция секретная, о ней никому нельзя рассказывать (запугивание).

Ваша карта заблокирована

Вам приходит СМС или сообщение в мессенджере, что ваша банковская карта заблокирована (страх потери). Для получения подробной информации предлагается перезвонить на определённый номер. Если вы перезвонили, вам сообщают, что в банке произошел технический сбой и для того чтобы карта заработала, вы должны сообщить её номер, пин-код или CVV/CVC/CVP код, а затем и код в СМС, который придёт на ваш номер. Если вы это сделаете, мошенники без труда спишут все ваши деньги.

С расчетного счёта вашей компании пытаются снять деньги

Мошенники атакуют не только граждан, но и организации. Главному бухгалтеру фирмы звонят из полиции (звонок от значимого лица) и сообщают, что его паспортные данные похитили и пытаются украсть деньги со счёта организации (страх потери или преследования). Поэтому надо срочно перевести деньги на безопасный счёт. Чтобы всё сделать правильно, надо установить на свой телефон специальное приложение.

АКЦИИ В ТЕЛЕГРАМ-КАНАЛАХ

Популярна мошенническая схема с акциями от банков и других известных компаний.

Например, можно случайно обнаружить у себя в подписках новый телеграм-канал, в котором используется логотип и изображение, похожее на узнаваемый брендинг банка.

Пользователям предлагают поучаствовать в акции, которая позволит получать от 50 до 70% кешбэка за покупки. Ссылка, которую оставляют мошенники, ведет на фишинговые сайты. Затем у клиентов банка запрашивают пароли или коды из СМС.

Не рекомендуем переходить по сомнительным ссылкам и делиться данными карты.

Обращаем внимание, что всю информацию об акциях и других предложениях следует искать только в официальных приложениях банков.

ИМИТАЦИЯ ГОЛОСА

Одна из популярных в последнее время схем обмана обязана своим появлением нейросетям.

Мошенники научились подделывать голоса родных потенциальной жертвы. Таким образом они вынуждают своих жертв совершать переводы денежных средств.

Чтобы вынудить человека сообщить необходимые сведения или совершить денежный перевод, злоумышленники могут выходить на контакт с ним от имени знакомых, родных или коллег, имитируя их голоса с помощью специальных программ.

Мошенники используют в подобных схемах нарезки из реальных старых голосовых сообщений жертвы. Сначала они получают доступ к аккаунту, затем начинают писать его контактам с просьбой перевести деньги. Историю о необходимости помощи преступники подкрепляют тем самым голосовым сообщением якобы от лица владельца аккаунта.

При возникновении сомнений необходимо связаться лично со знакомым, от имени которого звонили, и уточнить у него информацию.

В связи с участившимися в последнее время обращениями граждан в ФСБ России по фактам мошенничества - хищения их личных или кредитных средств неизвестными лицами с использованием подменных телефонных номеров, идентичных номерам телефонов доверия ФСБ России, приемной ФСБ России, справочного телефона ФСБ России, а также направлением по электронным мессенджерам фотографий «служебных удостоверений» Федеральная служба безопасности Российской Федерации информирует:

- НЕ ВЕРЬТЕ ЗВОНКАМ от так называемых сотрудников и следователей ФСБ России о том, что ВЫ являетесь подозреваемым (обвиняемым). Уведомление гражданина о привлечении в качестве подозреваемого (обвиняемого) осуществляется ИСКЛЮЧИТЕЛЬНО В ПИСЬМЕННОМ ВИДЕ И ВРУЧАЕТСЯ ЛИЧНО;

- сотрудники ФСБ России никогда не присылают гражданам копии своих служебных удостоверений;

- НЕ ВЕРЬТЕ ПРЕДЛОЖЕНИЯМ о необходимости получения кредита, перевода денег на «БЕЗОПАСНЫЙ СЧЕТ» или передачи их курьеру;

- ФСБ России НЕ ИСПОЛЬЗУЕТ личные сбережения или кредитные средства граждан для оказания помощи оперативным подразделениям в предупреждении и раскрытии преступлений;

- номера телефонов 8(495)224-22-22, 8(800)224-22-24, 8(495)224-70-69, 8(495)624-31-58 используются ИСКЛЮЧИТЕЛЬНО ДЛЯ ПРИЕМА ИНФОРМАЦИИ от граждан и организаций.

!!О чем нужно помнить, чтобы не стать жертвой мошенников?

1. Прежде чем перечислять деньги, важно убедиться, что информация достоверна.

2. Если объявление разместил или отправил в сообщении (в том числе голосовом) кто-то из ваших знакомых, обязательно дозвонитесь до этого человека и уточните, действительно ли требуется помощь.

3. Если вы решили пожертвовать деньги на благотворительность, выбирайте фонды, которые достойны доверия. Можно ориентироваться, например, на списки крупнейших фондов, которые публикуют рейтинговые агентства. В них включены только настоящие благотворительные организации, которые не первый год помогают людям.

Мошенники могут подделать и страницу фонда. Важно убедиться, что вы вводите данные банковской карты на безопасном сайте.

-проверьте адрес сайта — нет ли в нем ошибок или опечаток;
- в адресной строке браузера должно стоять https и значок закрытого замка ;
- небрежный дизайн или подозрительно;
- отсутствующие разделы меню могут указывать на то, что перед вами поддельный сайт.

4. Заведите отдельную дебетовую карту специально для переводов и оплаты покупок в интернете. Не держите на ней много денег — лучше каждый раз пополняйте ее ровно на ту сумму, которую собираетесь потратить. Тогда, даже если мошенники получат доступ к вашему счету, вы не лишитесь всех своих сбережений.

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.

ОБК ГУ МВД России по Саратовской области