

С какими мошенническими схемами можно столкнуться в 2024 году (данные МВД России)

Мошенничества в мессенджерах

Мошенничества в мессенджерах представляют собой разновидности фишинга.

Аферисты используют платформы мессенджеров из-за:

- удобства
- дешевизны поддержки
- невозможности создателей сервисов в полной мере контролировать пересылаемый контент.

Первое место по осуществляемым атакам занимает WhatsApp (принадлежит Meta признана в РФ экстремистской и запрещена), второе — Telegram.

Как это работает?

Смишинг (англ. SMiShing — от «SMS» и «фишинг») — основной способ обмана в мессенджерах, при котором мошенники рассылают сообщения, мотивирующее адресатов перейти по ссылке на поддельный сайт.

Наиболее распространенные темы — розыгрыши и конкурсы, распродажи товаров по низким ценам, а также информация о получении субсидий или социальных выплат. Затем аферисты узнают персональные сведения и данные банковских карт жертвы, вынуждают перейти по ложной ссылке для оплаты товаров или услуг.

Голосовые варианты фишинга: вишинг и претекстинг

Вишинг (англ. vishing — от voice (голос) + phishing) — атака при использовании методов социальной инженерии, но уже с помощью телефонного звонка. Мошенники маскируются под определенную организацию или сотрудника ИТ-службы.

Претекстинг (англ. pretexting) — атака, при реализации которой злоумышленник действует по заранее подготовленному сценарию. Обычно подразумевается предварительный сбор информации о жертве: день рождения, ИНН, номер паспорта либо последние цифры счета для того, чтобы не вызвать подозрений у адресата.

90% всех случаев кибермошенничеств совершается посредством телефона.

Наиболее часто применяется схема с «банковскими сотрудниками». Лжесотрудник, информирует жертву о проблемах с его банковской картой или сомнительных операциях и под предлогом решения вопроса узнает реквизиты или код подтверждения из банка.

Результативность таких атак в значительной мере зависит от умелого использования злоумышленниками методов социальной инженерии.

Еще одним вариантом преступного использования мессенджеров является взлом аккаунтов пользователей и подделка симкарт.

Мошенники имитируют документы на перевыпуск симкарт, а затем получают доступ к мессенджерам, контактам и личным кабинетам приложений. После они получают могут писать людям от лица того, кому раньше принадлежал номер.

Как распознать?

1. Отправитель или звонящий «давит» на эмоции, особенно на страх, и настаивает на срочности выполнения действий.
2. Письмо выглядит подозрительно: текст содержит ошибки или замены символов.
3. Отправитель, с которым долгое время не было контакта, о чем-то просит (например, срочно перевести деньги).
4. В случае попадания на фишинговый сайт нужно обратить внимание на его оформление, дату регистрации и контент.

Рекомендации по защите:

1. Проверяйте информацию о незнакомом номере на специальных ресурсах в интернете и, в случае отрицательных отзывов, не реагируйте на сообщения или звонки этого абонента.
2. Не открывайте подозрительные сообщения, сразу же удаляйте их и блокируйте автора.
3. Не переходите по ссылкам из подозрительных сообщений, а также не скачивайте файлы, которые прикреплены к ним.
4. Установите антивирусное ПО и регулярно обновляйте его.
5. Используйте надежные пароли, многофакторную аутентификацию, своевременно обновляйте мессенджеры.

Что такое информационная гигиена и почему её надо соблюдать?

С развитием цифровых технологий и началом информационной эры стало крайне важным соблюдение правил информационной гигиены.

Обилие и доступность распространяемой информации привели к тому, что в публичном поле можно столкнуться как с объективными сведениями, так и с ложью или манипулированием.

При этом такой обман могут использовать злоумышленники для управления не только конкретным человеком, но и общественным сознанием. То есть, они могут оказывать влияние на социальные процессы.

Правило №1.

В интернете нельзя никому доверять, надо всё проверять.

Разместить информацию в интернете может любой желающий из любой точки мира. Поэтому никогда не верьте на слово. Проверяйте информацию, постарайтесь составить полную картину произошедшего события, понять, какие есть подтверждения и доказательства.

Новости имеют сетевую структуру: появляются на новостных лентах крупных интернет-изданий, далее попадают в новостные агрегаторы, потом распространяются блогерами. То есть значительная часть новостей — это перепечатки.

Если инфоповод появился в крупных изданиях, распространился в блогосфере и на аналитических ресурсах, то вы легко найдёте и первоисточник, и дополнительные детали. Если же вы увидели видеоролик блогера, а в достоверных источниках информации о событии нет, то с большой вероятностью это фейк или постановка.

Правило №2

Если реклама заинтересовала — не спешите с решением о покупке.

Создать страничку в интернете несложно и недорого. А потом можно разместить на ней рекламу и постараться привлечь как можно больше посетителей. Ещё проще купить рекламу на агрегаторе новостей или у блогера.

На крупных интернет-ресурсах рекламные объявления проходят модерацию, но не проверку качества. Сложно привлечь к ответственности авторов недостоверной информации, размещённой на малоизвестных сайтах. Поэтому нужно самостоятельно проверять содержащиеся в рекламе факты.

Хорошей практикой может стать проверка информации о товаре по отзывам на крупных маркетплейсах. Как правило, на хороший товар будет порядка 100 положительных отзывов, но будут и отрицательные. Всегда найдётся несколько покупателей, которых товар разочарует.

Если вы выбираете подрядчика для строительства дома или ремонта, то найдите реальных клиентов компаний, к которым хотите обратиться, и посмотрите на качество работы. Только после этого можно заключать договор.

Правило №3

Ставьте под сомнение все сообщения в мессенджерах.

Не принимайте на веру присланные в мессенджеры сообщения, будь то родительские чаты или группы по интересам в социальных сетях.

Во-первых, даже знакомый человек может отправить вам непроверенные сведения. Во-вторых, его аккаунт могли взломать мошенники.

Всегда проверяйте полученную информацию и не переходите по ссылке, пока не удостоверитесь, что её действительно прислал ваш знакомый, и что она безопасна.

Прежде чем отреагировать на сообщение в мессенджере:

1. Оцените, не принесёт ли вред вам или вашим близким выполнение действия, о котором вас просят?

2. Подумайте, вызывает ли сообщение сильные эмоции: страх, любопытство, алчность, азарт, сострадание? Это признак мошеннического сообщения.

3. Оцените контекст переписки. Например, если от малознакомых людей приходит просьба проголосовать за ребёнка в конкурсе — это странно. Это типичная уловка мошенников для кражи аккаунтов в мессенджерах.

Правило №4

Будьте бдительны при просмотре фото и видео.

В качестве подтверждения реальности события нередко используются фото- и видеоматериалы. Однако им нельзя верить безоговорочно, поскольку они могут быть сделаны совсем в другое время и в другом месте.

Изображение может быть смонтировано. Более того, технология deepfake позволяет создавать фейковые фото и видео, которые очень сложно отличить от настоящих.

С 1 сентября в России вступили в силу ряд новых законодательных норм, среди которых:

Запрет на использование школьниками смартфонов на уроках, даже в образовательных целях.

Запрет на самостоятельную смену операторами связи тарифов без согласия клиентов.

Основные правила цифровой безопасности для родителей и их детей

Контролируемый доступ

Родители должны контролировать, какие сайты посещает ребёнок, и устанавливать фильтры для блокировки нежелательного контента.

Образование и предупреждение

Важно объяснить детям о возможных рисках в интернете, безопасных сайтах и общении в сети.

Конфиденциальность

Научите ребёнка важности защиты личной информации и объясните, какую информацию нельзя выкладывать в сеть.

Самоконтроль и ответственность

Дети должны уметь правильно принимать решения о том, что безопасно делать в интернете, что нет.

Мониторинг и сопровождение

Родители должны активно участвовать в онлайн-жизни детей, беседовать о происходящем в интернете и контролировать их активность.

Свод простых правил, соблюдение которых позволит сохранить в безопасности свой аккаунт на портале «Госуслуг»:

Используйте уникальный пароль.

Включите двухэтапную проверку входа.

Включите оповещения о входе в ваш аккаунт.

Задайте контрольный вопрос.

Включите вход с помощью электронной подписи.

По какой причине мошенники стремятся скомпрометировать учётные записи граждан на портале «Госуслуги»?

Основная цель: оформление различных кредитных продуктов в микрофинансовых организациях с помощью скомпрометированного личного кабинета пользователя.

При получении доступа к аккаунту пользователя на портале «Госуслуги» злоумышленники могут авторизоваться на сайтах различных микрофинансовых организаций.

Небольшие по размеру займы могут быть выданы даже в том случае, если произойдёт только авторизация через портал «Госуслуги», без предоставления каких-либо дополнительных данных.

Основным способом входа в личный кабинет на портале «Госуслуги» является код подтверждения из SMS-сообщения, который аферисты могут заполучить у пользователя под различными предложениями.

Повышение уровня цифровой грамотности населения и усиление мер безопасности на портале «Госуслуги» являются важными шагами для предотвращения подобных мошеннических схем.

Поменяли сим-карту — открепите номер от Госуслуг и мобильного приложения.

Киберпреступники приобретают старые сим-карты, которые уже были использованы и поступили в повторную продажу. Затем они используют эти сим-карты для восстановления доступа к учетным записям различных онлайн-сервисов.

Это может привести к утечке конфиденциальной информации, такой как паспортные данные, информация о недвижимости и автомобилях, и другие личные данные.

Как избежать многомиллионного кредита, взятого на ваше имя другим человеком?

Первым делом открепите неиспользуемый номер телефона от портала «Госуслуг», онлайн-банка и других своих аккаунтов.

Сделать это самостоятельно можно, если сим-карта, которой вы не планируете больше пользоваться, все еще установлена в вашем телефоне. Связано это с тем, что на этот номер придет код, подтверждающий ваши действия.

Сменить номер телефона достаточно просто, на портале «Госуслуги» нужно перейти в раздел «Настройки и безопасность» (<https://sba.yandex.net/redirect?url=https%3A//lk.gosuslugi.ru/settings/account&client=znatoki&sign=1a58afe3da783f73a0161f48c5446229>) и нажать «Изменить» напротив прикрепленного номера телефона.

Если же сим-карты на руках у вас уже нет – потеряли или выбросили за ненадобностью, – сменить номер на портале «Госуслуг» самостоятельно не получится. Вам необходимо обратиться в МФЦ.

Отдел по вопросам общественной безопасности и профилактики правонарушений Администрации города Ханты-Мансийска