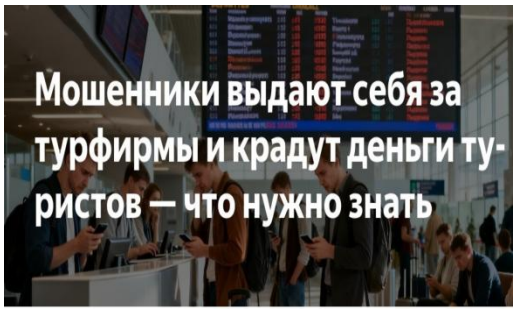
Обзор мошеннических схем с использованием информационных технологий, мобильной связи и сети Интернет

Центр компетенций
по информационной безопасности

Апрель 2026 г.

Содержание:

Мошенники используют тревожность туристов для хищения денег.



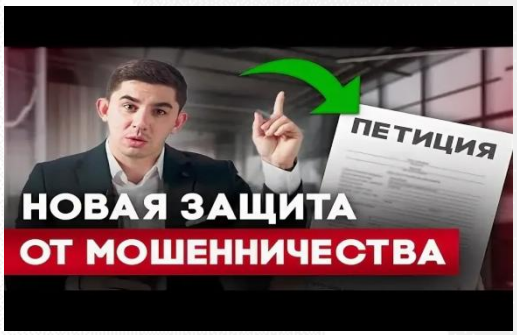
На фоне обострения ситуации на Ближнем Востоке активизировались мошенники, которые используют тревожность туристов для хищения данных и средств, предлагая якобы помощь или компенсации. Так, одной из распространенных схем стали фишинговые письма и сообщения о возврате средств за отмененные рейсы. Мошенники рассылают уведомления от имени авиакомпаний или турагентств и предлагают перейти по ссылке для получения компенсации. На поддельных сайтах у пользователей запрашивают персональные и банковские данные, после чего получают доступ к их счетам.

Также фиксируются случаи создания фейковых туристических агентств, которые предлагают «экстренные» билеты для пассажиров отмененных рейсов. Злоумышленники требуют предоплату за быстрое решение проблемы, однако после получения денег прекращают связь и не оказывают никаких услуг.

Отдельное направление — поддельные сервисы эвакуации. Мошенники могут предлагать услуги по «эвакуации» из зоны конфликта или экстренной транспортировки в другие страны. Они создают фальшивые сайты или группы в социальных сетях, где просят внести депозит или полную оплату за услуги. После получения средств они прекращают контакты, оставляя жертву без помощи.

https://iz.ru

Общественные инициативы и петиции для кражи персональных и учетных данных граждан.



Мошенники активно используют тему общественных инициатив и петиций для кражи персональных и учетных данных граждан. Созданные ими поддельные интернет-ресурсы, имитируют сервисы сбора общественных петиций, в том числе обращений к руководству страны.

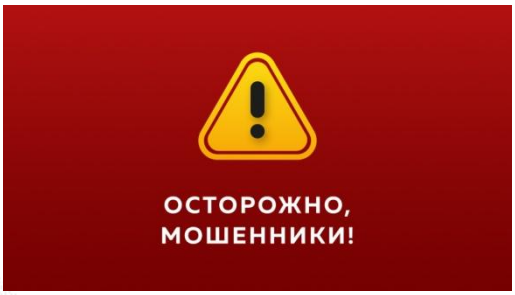
Все выявленные ресурсы имеют практически идентичную структуру, визуальное оформление и функционал по взаимодействию с пользователем. На главных страницах размещается псевдореестр обращений, основная масса петиций направлена на поддержку участников боевых действий или увековечивание памяти погибших в зоне СВО.

Ключевой элемент мошеннической схемы — предложение подписать петицию через систему «Госуслуги» по предложенной ссылке. При попытке

авторизации пользователь перенаправляется на фишинговую страницу, которая с высокой точностью копирует интерфейс официального портала. Введенные логин и пароль, а также иные персональные данные напрямую перехватываются преступниками.

https://www.gazeta.ru

Мошенники начали атаковать российские компании под видом трудовых инспекций и других контрольно-надзорных органов.



Российским компаниям направляются письма и уведомления о якобы выявленных признаках теневой занятости, нарушениях трудового законодательства или несоответствии отчетности. Документы оформляются с использованием официальной символики, поддельных реквизитов и ссылок на нормы закона. Ключевым элементом этой схемы является запугивание якобы внеплановой выездной проверкой и угрозой крупных штрафов. Также руководству и бухгалтерии предлагают срочно предоставить кадровые документы, штатные расписания, договоры с сотрудниками, а также перейти по указанной в письме ссылке или связаться с инспектором. В ряде случаев мошенники требуют оплатить госпошлину, сбор за рассмотрение материалов или предварительный административный штраф через QR-код. Именно на этапе оплаты и происходит хищение средств либо компрометация банковских данных организации.

https://tass.ru

Новая схема обмана пользователей Telegram с «секретным чатом».

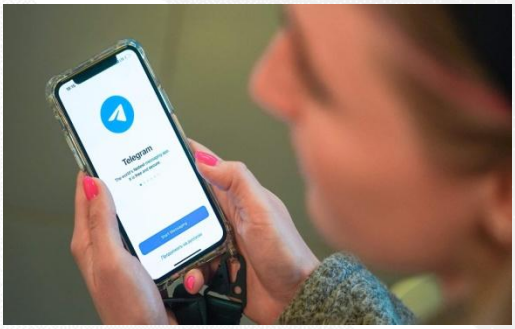


Схема кражи аккаунта Telegram от лица поддержки мессенджера путем направления фишинговой ссылки в секретный чат. Мошенники не случайно используют именно секретные чаты. Обычно такую переписку нельзя удалить, в ряде случаев не удается сделать скриншот или переслать сообщение другому человеку или в реальную службу поддержки Telegram.

Пользователи получают сообщение якобы от мессенджера о входе с другого устройства и просьбой перейти по ссылке для подтверждения или опровержения. Другой вариант обращения к пользователю - от лица поддержки мошенники пишут о том, что им якобы поступил запрос на удаление учетной записи. Для «отмены» запроса надо перейти по ссылке для авторизации. В противном случае аккаунт якобы будет удален. После перехода по ссылке и

ввода логина и пароля от своего аккаунта жертва передает доступ к нему злоумышленникам вместе с личными данными, переписками, фото, видео и аудиозаписями. Эта информация в дальнейшем может быть использована для обмана как самой жертвы, так и ее близких.

https://tass.ru

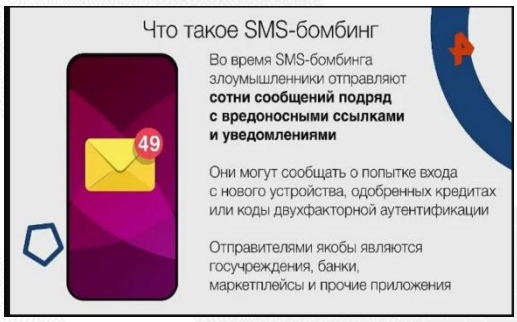
Мошенники начали добавлять россиян в фальшивые чаты поликлиник.

Мошенники начали добавлять россиян в фальшивые чаты поликлиник и под предлогом подтверждения прикрепления к медучреждению выманивать их личные данные. Злоумышленники отправляют ссылку на якобы анкету для подтверждения данных. Однако эта ссылка ведет на фишинговый сайт.

Если жертва переходит по ссылке, на ее устройстве может автоматически начать скачиваться и устанавливаться вредоносное программное обеспечение. Таким образом, злоумышленники могут завладеть управлением мобильным устройствам и получить доступ к личным данным.

https://ria.ru

Новая схема - «СМС-бомбинг».

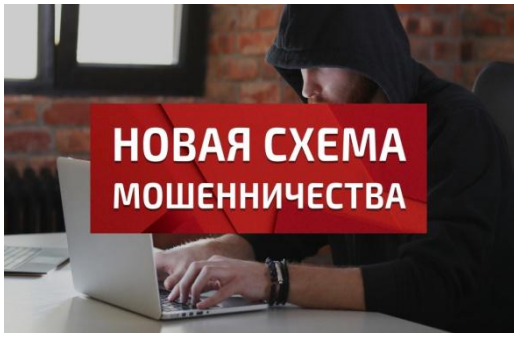


Мошенники придумали новую двухэтапную схему обмана, получившую название «СМС-бомбинг». Суть схемы сводится к тому, что вначале жертве поступает огромное количество различных СМС, которые могут имитировать взлом сразу нескольких сервисов и аккаунтов, например «Госуслуг», мессенджеров или банковских приложений, используя для этого специальные программы, причем адреса отправки очень похожи на официальные. Цель злоумышленников – вызвать панику, заставить его действовать быстро и необдуманно.

Далее жертве поступает звонок от мошенников, в ходе которого злоумышленники представляются сотрудниками сотовых операторов, банков или органов государственной власти заявляют о предполагаемом взломе аккаунтов жертвы, а для восстановления доступа злоумышленники требуют назвать код из СМС или push-уведомления, паспортные данные или данные банковской карты. В результате пользователь может случайно передать злоумышленникам доступ к своим аккаунтам или финансовым данным.

https://www.gazeta.ru

Коды из СМС в прошлом - мошенники стали просить назвать последние цифры номеров телефонов.



Если раньше аферисты связывались с жертвами, чтобы выудить коды из СМС и взломать аккаунт на Госуслугах или личные банковские кабинеты, то сейчас на это уже никто не ведется. В ответ на это злоумышленники стали просить назвать последние 4 цифры номера телефона, который недавно совершил входящий вызов. Устроено все следующим образом.

Мошенник под разными предлогами связывается с жертвой в соцсетях или мессенджере (например, запись на маникюр, фотосессию или другую услугу). В рамках беседы аферист обещает позвонить с того или иного номера телефона для уточнения деталей. Пользователю действительно поступает звонок с неизвестного номера, который сразу сбрасывается. Мошенник в переписке просит жертву назвать последние две или четыре цифры только что звонившего номера, якобы чтобы убедиться, что номер клиента набрали правильно.

Если жертва назовет последние цифры номера телефона, то мошенник сможет использовать их для входа в личные кабинеты, например, в финансовых сервисах, чтобы затем похитить денежные средства. Подобным образом «увести» могут в том числе аккаунт на маркетплейсе, электронную почту, профиль в онлайн-магазине или аккаунт в мессенджере.

https://www.anti-malware.ru

Блокировка iPhone и iPad через вредоносные «клоны» Telegram якобы для обхода замедлений.

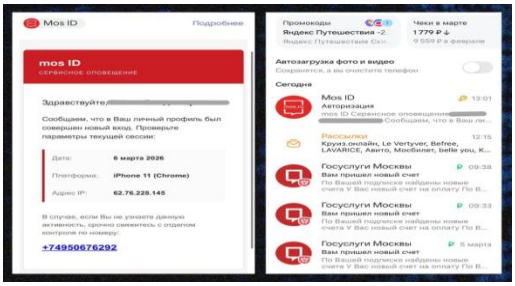
Злоумышленники активно используют информацию о блокировке Telegram. В рекламных объявлениях они предлагают установить якобы улучшенные версии мессенджера с дополнительными функциями, среди которых указываются встроенный VPN, анонимный номер, режим инкогнито и Premium-подписка без оплаты. Среди мошеннических программ фигурируют названия ToxicGram, DarkGram, HakoGram, HoloGram, AstroGram или Doxogram.

Потенциальным жертвам через телеграм-бота предлагают установить мод. Пользователю объясняют, что приложение отсутствует в App Store, поэтому его нужно скачать, авторизовавшись через сторонний Apple ID. Для этого злоумышленники передают логин и пароль от чужой учетной записи.

После того как человек привязывает устройство к этой учетной записи, мошенники блокируют аккаунт и сам гаджет. На экране появляется сообщение с контактами для связи, где злоумышленники требуют деньги за разблокировку устройства.

https://www.cnews.ru

Мошенники используют рассылку от имени портала mos.ru.



Мошенники начали рассылать пользователям сообщения (по СМС или через мессенджеры) о якобы входе в учетную запись портала mos.ru с неизвестного устройства. В сообщении указывается номер телефона, по которому предлагается срочно перезвонить в службу технической поддержки для блокировки подозрительной активности. Однако при обращении по нему отвечают злоумышленники, которые под видом сотрудников портала пытаются выманить у него персональные данные, логины, пароли или информацию о банковских картах.

https://ria.ru

Всплеск мошеннических рассылок под видом писем от медицинских учреждений.

Пользователю приходит письмо с адреса, который пытается мимикрировать под легитимную почту государственной организации или медучреждения. В нём предлагается подтвердить актуальность обслуживания в поликлинике: для этого нужно перейти по ссылке.

Если кликнуть по ней, откроется сайт, похожий на официальный, с формой ввода номера телефона и кнопками «Продлить» и «Открепить». Вне зависимости от выбора пользователь получает номер талона, который предлагается отправить в регистратуру, кликнув по кнопке.

Цель злоумышленников — получить телефонные номера пользователей для использования в дальнейших атаках.

Далее схема развивается по одному из сценариев:

- после «отправки талона» появляется предупреждение о том, что по указанному номеру якобы произошёл вход на портал государственных услуг, и нужно дождаться звонка от «специалиста для проверки защиты аккаунта»;
- после ввода номера пользователь видит сообщение о скором звонке из регистратуры.

Во всех сценариях звонки поступают не от специалиста для проверки защиты аккаунта или работника регистратуры, а от злоумышленников, которые попытаются получить доступ к аккаунтам жертвы.

https://ria.ru

Мошенничество с доставкой техники.

Злоумышленники звонят гражданам и информируют, что на их имя и адрес заказана доставка товаров из магазина электроники. Для убедительности они озвучивают личные данные жертвы. После того как «клиент» подтверждает информацию, мошенники говорят, что на телефон скоро придет код, который нужно продиктовать для завершения оформления или передачи заказа. В действительности этот код позволяет мошенникам получить доступ к аккаунту или выполнить перевод денежных средств.

Если жертва пытается узнать, что именно было заказано, через какой сайт и когда производилась оплата, мошенники игнорируют эти вопросы и переводят разговор на другую тему, торопя жертву при помощи следующих фраз: «курьер уже едет», «сейчас потеряете доставку».

https://ria.ru

Обман пользователей онлайн-игр.

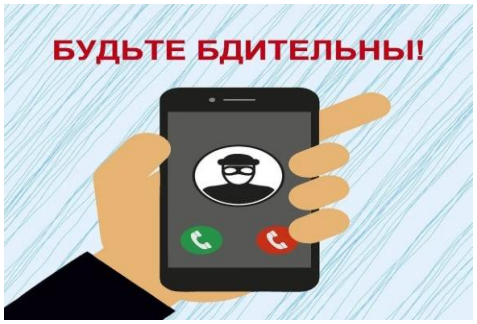
Мошенники внедрили новую схему обмана пользователей онлайн-игр, убеждая их пройти «аутентификацию».

Злоумышленники пишут игрокам в Telegram, представляются администраторами и утверждают, что для продолжения пользования игрой необходимо подтвердить учетную запись. Для этого они присылают ссылку и просят связаться по телефону или видеосвязи.

Не ожидая подвоха, потенциальная жертва связывается с собеседником, который просит включить экран, а затем входить в различные приложения, в том числе банковские. Параллельно с этим человеку приходят СМС-уведомления, которые являются ключом для списания денег. Таким образом, мошенники получают полный доступ к финансовой информации и средствам своих жертв.

https://iz.ru

Преступления под влиянием мошенников!



В России участились случаи, когда люди совершают преступления под влиянием мошенников:15-летний подросток взорвал банкомат в Москве, молодая девушка пыталась забить молотком пенсионерку, думая, что помогает спецслужбам, а 20-летний футболист убил женщину — мошенники убедили его пробраться в квартиру к жертве и забрать из сейфа деньги. Кроме того, злоумышленники принуждают подростков «похищать» самих себя и вымогают выкуп у их родителей. Этот всплеск связан с эволюцией телефонного мошенничества: преступники, управляя поведением жертв, вовлекают их во всё более сложные схемы.

Все телефонные мошенники действуют примерно по одной схеме. Они внушают людям, что их ожидает суровое наказание за некое вымышленное преступление и предлагают «сотрудничать со следствием» — выступать в качестве якобы внештатных агентов в интересах государства. А на самом деле ставят перед ними преступные задачи.

Несовершеннолетних вовлекают через сочетание давления и манипуляции. Часто используются легенды о «проблемах с законом», «угрозе родителям», «утечке персональных данных» или «участии в спецоперации». В иных случаях обещают, что они смогут заработать «легкие деньги», практически ничего не делая.

Злоумышленники могут шантажировать компрометирующей информацией — угрожать опубликовать личные данные, записи или изображения, которые могут навредить репутации жертвы. Это может быть, как реальная информация, так и сфабрикованная. Подростков, как правило, вовлекают в криминальные схемы через соцсети, мессенджеры и онлайн-игры.

https://iz.ru

Обман вернувшихся из зарубежных поездок россиян.

Мошенники придумали новый способ обмана, нацеленный на тех, кто ездит за границу. Через некоторые время после возвращения гражданину поступают звонки или сообщения в мессенджеры с незнакомых номеров. Собеседники представляются сотрудниками госорганов и заявляют, что человек якобы контактировал с запрещенной или нежелательной организацией, а также мог нарушить закон. По этой лже-причине ему «грозит проверка»,

блокировка счетов и другие последствия. Аферисты пугают жертву уголовной ответственностью и тут же предлагают быстрое решение.

Мошенники просят перевести деньги на «безопасный счет», назвать данные карт и счетов, установить «спецприложение» или перейти по ссылке. Это все та же схема «звонок от службы безопасности», только адаптированная под поездки за рубеж.

https://tass.ru

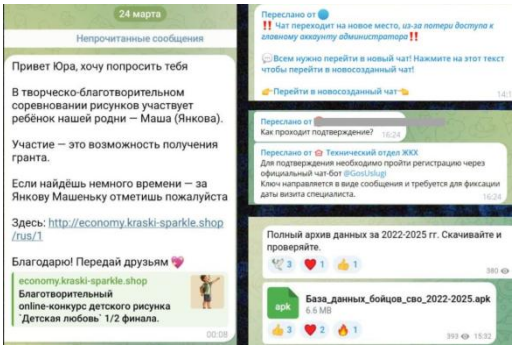
Мошенники заставляют геймеров загружать вредоносные приложения.

Мошенники обманывают подростков-геймеров, заманивая их возможностью бесплатно получить уникальные предметы в играх через установку вредоносных приложений. В мессенджерах появляются каналы и чаты для фанатов популярных игровых проектов. В них предлагают то, что всегда вызывает интерес у молодой аудитории: бесплатные модификации, уникальные улучшения, ускоренную «прокачку» персонажа и редкие предметы. Организаторы таких чатов серьезно подходят к оформлению и делают всё, чтобы не вызвать подозрений. После этого, подростка ведут «по цепочке», заставив его подписаться на несколько тематических каналов, чтобы тем самым отбросить все подозрения насчет возможного мошенничества.

Финальный шаг - загрузка файла не из официального магазина приложений, а напрямую через бота в мессенджере. Пользователя просят разрешить установку расширения из неизвестных источников, а также, разумеется, отключить системные предупреждения и антивирус. На самом деле в этот момент на устройство устанавливается вредоносное приложение. Под видом игровой модификации скрывается троян, который после установки получает доступ к СМС, уведомлениям, а иногда - к банковским приложениям. Он может перехватывать коды подтверждения, передавать данные третьим лицам, использовать телефон для дальнейшего распространения вредоносного ПО. Опасность данной мошеннической схемы скрывается в том, что всё происходит не на отдельных ресурсах, а в привычной «среде обитания» - мессенджерах. Мессенджер не воспринимается как источник угрозы, он ассоциируется с друзьями, интересами и хобби: именно это доверие и используют мошенники. Здесь нет давления, нет срочности, нет запугивания - только интерес и любопытство.

https://ria.ru

Зачем мошенники «угоняют» аккаунты в мессенджерах?



Мошенникам нужен не сам аккаунт, а доверие, которое к нему уже «привязано». Знакомое имя, привычная фотография, история переписки и круг контактов дают преступникам значительные возможности.

После захвата аккаунта мошенники действуют сразу по нескольким направлениям.

Рассылают вредоносные файлы и фишинговые ссылки по списку контактов и в общие чаты.

Используют профиль для социальной инженерии: переводят людей в поддельные боты, выманивают коды из СМС, получают доступ к банковским и государственным сервисам.

Ищут в диалогах финансовую, личную или компрометирующую информацию для шантажа или получения доступа к платежным средствам. Главная опасность в том, что чужой аккаунт позволяет атаковать не одного человека, а его родственников, коллег, родительские и домовые чаты. Именно поэтому мошенники так настойчиво охотятся за кодами авторизации и доступом к мессенджерам.

https://tass.ru

Рекомендации по мерам защиты от телефонного и интернет-мошенничества!

1. Не сообщайте личную информацию о себе неизвестным вам людям по телефону, через мессенджер или по электронной почте.
2. Не отправляйте копии, фото своих документов, не озвучивайте реквизиты банковской карты, код из СМС и иную персональную информацию.
3. Не переходите по сомнительным ссылкам.
4. Используйте антивирус на своих мобильных устройствах.
5. Используйте сложные и разные пароли для разных приложений и систем.
6. Не устанавливайте приложения на телефон из неавторизированных магазинов и внимательно следите за настройками конфиденциальности.
7. Критически относитесь к любым входящим сообщениям и звонкам от неизвестных абонентов. Если во время диалога возникают хотя бы малейшие сомнения, лучше прекратить беседу и не перезванивать на незнакомый номер.
8. Если вы получили подозрительное сообщение от якобы знакомого, обязательно свяжитесь с человеком напрямую по известному вам номеру телефона.
9. Ограничьте доступ к своему номеру телефона в настройках приватности в мессенджерах и социальных сетях.
10. Информацию о социальных выплатах, компенсациях, налоговых вычетах и перерасчетах проверяйте только на официальных сайтах ведомств, портале «Госуслуги» или в МФЦ.
11. Избегайте регистрации на неизвестных ресурсах и не вводите на них личные данные.
12. Всегда проверяйте репутацию неизвестных сайтов.
13. Воздержитесь от использования ботов в мессенджерах, если вы не можете достоверно установить их владельцев.
14. Критично относитесь к информации в мессенджерах и социальных сетях, где предлагают получить различные подарки, бонусы или принять участие в беспроигрышных лотереях, акциях, особенно если для участия необходимо передать личную информацию. Злоумышленники активно используют подобные сообщения для вовлечения в мошеннические схемы, а полученную личную информацию используют для дальнейших противоправных действиях или продажи.