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

Центр компетенций
по информационной
безопасности

Января 2026 г.

Содержание:

Мошенники придумали новую схему обмана с «налоговой инспекцией».

Мошенники звонят, представляются сотрудниками ФНС и сообщают, что человек находится «на проверке». Поясняют, что, по данным налоговой, расходы сильно превышают доходы и необходимо в этом разобраться. Для правдоподобности называют адрес ближайшей инспекции, куда в ближайшее время надо подойти с документами, иначе будут штрафы, доначисления и даже судебные разбирательства.

После этого через какое-то время поступает еще один звонок – якобы для записи в налоговую инспекцию на определенное время. Для подтверждения временного слота нужно назвать данные из СМС, которое придет с портала «Госуслуг».

Все это лишь с одной целью – получить доступ к личному кабинету портала «Госуслуг» жертвы. А после этого начнется основной этап обмана. Жертве сначала звонит якобы «оператор колл-центра с Госуслуг». Он переводит на «отдел по борьбе с телефонным мошенничеством». Человека пугают тем, что мошенники уже якобы получили доступ к банковским счетам и вот-вот отправят деньги на финансирование ВСУ, что это уже уголовно наказуемое деяние, госизмена с вытекающими последствиями. Чтобы этого избежать, нужно «задекларировать» все свои деньги и положить их на «безопасный счет» в Центробанке. Если человек поддается на уговоры и давление мошенников, то денежными средствами завладевают мошенники.

https://www.kp.ru

Как мошенники воруют деньги у водителей.

В России участились случаи мошенничества с вредоносными приложениями, которые маскируются под сервисы для определения дорожных камер. Жертвами становятся водители, скачивающие якобы бесплатные «антирадары».

Схема обмана проста: злоумышленники распространяют вирусы через пиратские сайты и мессенджеры под видом приложений с названиями: DPS_RADAR, GDEDPS, Антирадар, Антирадар_камеры, PDS-Radar.

После установки такого приложения вредоносная программа получает доступ к банковским приложениям и SMS на телефоне, что позволяет мошенникам незаконно списывать деньги со счетов пользователей.

https://vestitula.ru

Мошенники предлагают фиктивные зимние скидки на ЖКХ.

Сначала мошенники проводят «информационный» звонок, представляясь сотрудниками соцзащиты или районных управ. Они сообщают о якобы введении специальных «зимних» скидок на оплату ЖКХ и предлагают оформить соответствующие льготы.

Однако для получения льгот мошенники под предлогом «идентификации личности» или «привязки лицевого счета» запрашивают у гражданина одноразовые пароли из СМС, которые на самом деле являются кодами подтверждения банковских операций. Все время разговора с жертвой преступники создают иллюзию официального обращения, ссылаясь на несуществующие нормативные акты о сезонных льготах.

https://www.ria.ru

Мошенничество с «совместным фото».

Мошенники стали рассылать россиянам от лица знакомых сообщения с подписью «Смотрю на фото, вспоминаю тебя», под которой размещена ссылка, якобы ведущая на фотографию. Мошенники используют нейронные сети для подделки аватаров знакомых и близких.

При помощи фишинговой ссылки преступники заражают устройство пользователя-жертвы, устанавливая на него вредоносный файл. Он может перехватывать и отправлять СМС, собирать с устройства данные о финансовых операциях, похищать деньги с банковских счетов пользователя.

Кроме того в преддверии Нового года мошенники придумали схему обмана россиян, предлагая сыграть в «тайного Санту». Аферисты рассылают в соцсетях ссылки с сообщением «Нажми, чтобы узнать, кто тебя поздравил». После клика жертве на устройство устанавливается вирусное ПО, которое также позволяет мошенникам получить доступ к личным данным человека.

https://ria.ru

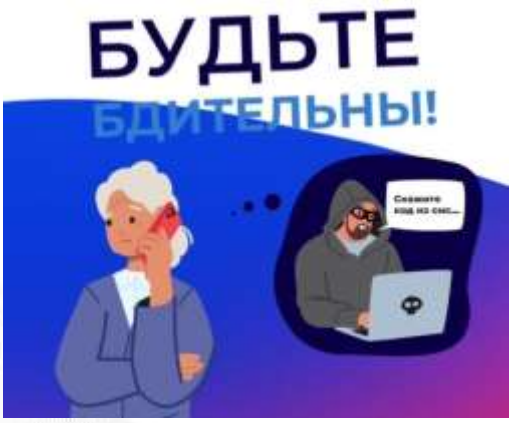
Мошенники придумали новую многоролевую схему обмана с обучающими курсами.

Мошенники разработали новую схему обмана. Теперь они предлагают гражданам пройти обучающие курсы на IT-специалистов, а после регистрации на учебу, угрожают уголовной ответственностью.

Сначала мошенники связываются с жертвой под видом IT-специалистов и предлагают пройти обучающие курсы. В ходе общения, якобы для регистрации на обучающей платформе они выманивают код из СМС. После с человеком связываются лжесотрудники портала «Госуслуги», которые сообщают о взломе аккаунта. Для большей убедительности жертве звонит якобы сотрудник банка и заявляет, что его деньги находятся под угрозой

хищения. Через несколько минут с человеком связывается псевдосотрудник спецслужб и обвиняет его в финансировании запрещенных организаций и угрожает уголовной ответственностью. Человек, поддавшись панике, начинает следовать полученным инструкциям и в итоге теряет свои деньги переведя их на «безопасный счет».
https://www.vesti.ru

Мошенники начали обманывать россиян под предлогом перерасчета пенсии.



Мошенники начали обзванивать пенсионеров, представляясь сотрудниками Пенсионного фонда России и предлагая перерасчет пенсии за 2016–2018 годы. Злоумышленники в ходе разговора называют персональные данные жертвы и рассказывают о якобы положенном перерасчете. Далее они предлагают пройти «перерегистрацию» в Пенсионном фонде, для этого они называют первые цифры банковской карты человека и просят назвать остальные, а затем спрашивают код, который пенсионер получает в СМС. После передачи кода мошенники получают доступ к банковской карте жертвы и могут снять с нее все средства.
https://ria.ru

Мошенники массово блокируют банковские карты россиян и вымогают деньги.

Россиян массово обманывают с помощью новой схемы через блокировку карты. Мошенники используют личные данные: фамилию, имя, отчество, номер телефона и дата рождения, которые легко берутся из слитых баз для блокировки банковской карты, а затем пугают людей, чтобы получить доступ к деньгам.

Схема выглядит следующим образом. Злоумышленники звонят в банк и, представляясь жертвой, называя личные данные, сообщают, что потеряли телефон. По внутреннему правилу, банк обязан заблокировать карту, если эти данные совпадают, считая это достаточным основанием для принятия срочных мер безопасности.

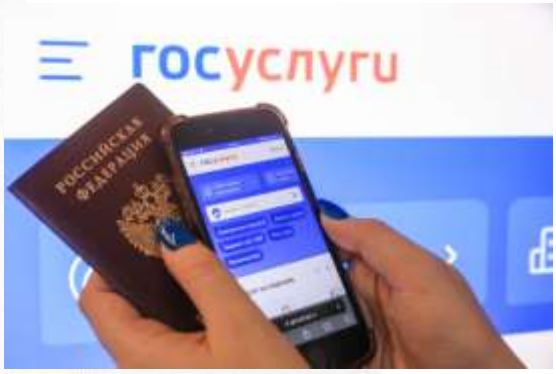
Ничего не подозревающий человек внезапно получает уведомления от одного или нескольких банков, что его карты заблокированы. Проверка статуса в приложении подверждает информацию — карты заблокированы

Сразу после блокировки мошенники связываются с жертвой и в крайне агрессивной манере начинают угрожать. Мошенники заявляют, что блокировка карты — это цветочки. Настоящий ад будет дальше, обещают запугивать родственников, публиковать данные жертвы и родственников в интернете, в том числе от имени жертвы, обещают проблемы с полицией. Но всего этого можно избежать — достаточно заплатить.

Разумеется, если человек платит, то преступники не останавливаются. Они могут требовать еще, продолжить давление, а то и вовсе заявить, что деньги ушли на счета, связанные с террористами и экстремистами, поэтому если жертва не отдаст всё или не совершит какое либо их указание, то может быть привлечено к уголовной ответственности за государственную измену.

https://www.banki.ru

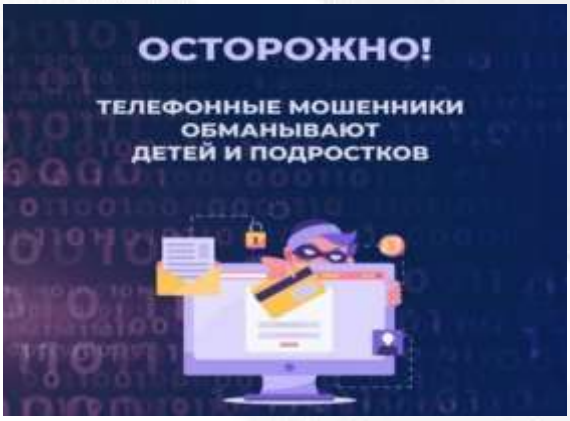
Россиян предупредили о новой схеме мошенничества с выплатами в декабре.



Мошенники от имени «Госуслуг» отправляют россиянам сообщения в мессенджерах о якобы возможности получить выплату в размере 15 тысяч рублей в декабре. В сообщении информируют, что выплату могут получить граждане РФ старше 18 лет. Для этого им «необходимо подать заявку» на официальном сайте «Госуслуги», перейдя по ссылке в сообщении. Попытавшихся получить обещанную выплату аферисты подписывали на мошеннические каналы. В них пользователям предлагали нелегальное казино, фальшивые инвестиционные инструменты. Кроме того, злоумышленники устанавливали на устройства жертв вредоносное программное обеспечение.

https://www.gazeta.ru

Россиян предупредили о способе, которым мошенники обманывают школьников.



Отмечается существенный рост числа случаев обмана, направленных на школьников, их родителей и сотрудников образовательных учреждений. В условиях сезонных массовых респираторных заболеваний мошенники звонят от имени школьной медсестры и сообщают о необходимости срочного медосмотра для допуска к занятиям. Под этим предлогом, они пытаются выманить код из СМС от учетной записи на «Госуслугах» или в банковском приложении. В других случаях они пытаются заставить

жертву пройти онлайн-регистрацию по фишинговой ссылке под предлогом «срочного медосмотра».

https://ria.ru

Обман с «подработкой» на продаже подарочных сертификатов.

Мошенники начали активно использовать схему обмана под видом удаленной подработки, связанной с продажей подарочных сертификатов. Они размещают объявления о простой удаленной работе в группах и каналах в мессенджерах. После отклика человека переводят в отдельную переписку или беседу и предлагают заработок на продаже подарочных сертификатов через онлайн-площадки.

Исполнителю отводится роль посредника: он принимает оплату от покупателя, оставляет себе небольшой процент, а остальную сумму перечисляет третьим лицам.

При этом покупателю передается недействительный, либо нерабочий сертификат. После появления претензий организаторы схемы обещают уладить ситуацию и компенсировать ущерб, однако затем прекращают общение, удаляют переписки и оставляют человека один на один с обманутыми покупателями.

В результате вся ответственность ложится на исполнителя, который вынужден либо возвращать деньги за свой счет, либо рискует быть привлеченным как соучастник противоправных действий.

https://iz.ru

Мошенники в преддверии Нового года изобрели несколько схем обмана.

Злоумышленники, представляясь агентами авиакомпаний или ОАО «РЖД», совершают массовые звонки, выбирая прицельно жителей Москвы, Санкт-Петербурга и других крупных городов-миллионников. Представляясь сотрудниками перевозчиков, они предлагают купить льготные билеты по «особой субсидированной цене». Затем для оформления «льготы» под предлогом подтверждения маршрута и паспортных данных у абонентов выманивают конфиденциальную информацию, персональные данные или просят немедленно внести предоплату на резервирование места.

https:/vazhno/news.ru

Мошенники заводят фейковые аккаунты в мессенджерах, где публикуют информацию о якобы распродаже красной рыбы и икры по привлекательно низким ценам. Для

оформления заказа злоумышленники требуют от своих жертв совершить полную предоплату, а затем, после того как деньги поступают, просто перестают выходить на связь, удаляя аккаунт в мессенджере.

https://iz.ru

Злоумышленники посылают работникам компаний СМС якобы от службы доставки с сообщением, что один из контрагентов компании отправил им подарок, но курьер не смог дозвониться. В сообщении предлагается связаться с курьером по указанному номеру напрямую. Для жертвы это создает видимость доверия и делового контекста. Информацию о контрагентах и клиентах мошенники собирают из открытых источников, включая сайт самой компании. После установления контакта преступники могут выманить персональные данные и конфиденциальную информацию, включая коды из СМС, а также убедить жертву оплатить различные сборы или перейти на фишинговый сайт, имитирующий портал службы доставки.

https://www.rbc.ru

Рекомендации по мерам защиты от телефонного и интернет-мошенничества!

1. Никогда и никому, особенно незнакомым людям, не отправляйте копии, фото своих документов, не озвучивайте полные реквизиты банковской карточки, особенно трехзначный код на обороте, код из СМС и иную персональную информацию.
2. Не переходите по сомнительным ссылкам.
3. Используйте антивирус на своих мобильных устройствах.
4. Используйте сложные и разные пароли для разных приложений и систем.
5. Не устанавливайте приложения на телефон из неавторизированных магазинов и внимательно следите за настройками конфиденциальности.
6. Критически относитесь к любым входящим сообщениям и звонкам. Если во время диалога возникают хотя бы малейшие сомнения, лучше прекратить беседу и не перезванивать на незнакомый номер.
7. С осторожностью относитесь к различным предложениям быстрого заработка, легкого выигрыша, больших дивидендов и т.д.
8. Информацию о социальных выплатах проверяйте только на официальных сайтах ведомств, портале «Госуслуги» или в МФЦ.
9. Избегайте регистрации на неизвестных ресурсах и не вводите на них личные данные.
10. Всегда проверяйте репутацию неизвестных сайтов.