ГУ МВД РОССИИ ПО СВЕРДЛОВСКОЙ ОБЛАСТИ

МИНИСТЕРСТВО СОЦИАЛЬНОЙ ПОЛИТИКИ СВЕРДЛОВСКОЙ ОБЛАСТИ

ГКУ СОН СО «ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ ЦЕНТР СОЦИАЛЬНОЙ ПОМОЩИ»

**Дайджест информационных материалов по профилактике мошеннических действий**

I квартал 2025 года

2025

ГКУ СОН СО «Организационно-методический центр социальной помощи»

Дайджест информационных материалов по профилактике мошеннических действий I квартал 2025 года – Екатеринбург. – 2025. – 20 с.

Дайджест информационных материалов составлен по публикациям на официальных ресурсах ОМЦСП в сети интернет [http://uralsocinform.ru/](https://vk.com/away.php?to=http%3A%2F%2Furalsocinform.ru%2F&cc_key=), <https://vk.com/omcspso> ,обзоров прессы, информации от правоохранительных органов. Предназначен руководителям и сотрудникам организаций социального обслуживания для использования в практической деятельности, а также работе с получателями социальных услуг.

В разделах дайджеста обобщены и систематизированы сведения о новых видах и способах мошеннических действий в отношении граждан. Даны методы настройки оборудования, способы предотвращения и алгоритмы реагирования не непредвиденные ситуации. Приведены примеры деятельности законодательной и исполнительной власти, направленной на решение проблем.

Редакторы-составители: сотрудники ГКУ СОН СО «Организационно-методический центр социальной помощи» И.А. Киселев, И.П. Ризничок.

СОДЕРЖАНИЕ

Раздел 1 Новые способы действий злоумышленников 4

Раздел 2 Рекомендации по защите 11

Раздел 3 Меры государства 16

Раздел 4 Обучающие мероприятия 20

1. **Новые способы действий злоумышленников**

Вредоносное программное обеспечение с расширением .apk.

Продолжается (<https://t.me/cyberbezopas95/289> ) рассылка в мессенджере Telegram вредоносного программного обеспечения с расширением .apk. Рассылка направлена на разные категории граждан, включая военнослужащих.

✈️Чаще всего злоумышленники направляют файлы, сопровождая их вопросом: «Это ты на видео?», также слово «видео» в разных вариациях используется в названии файла.

🎁При открытии файла происходит установка приложения, после чего устройство может быть заражено трояном Mamont (https://t.me/kasperskylab\_ru/5735), считывающим push-уведомления, СМС сообщения и фотографии из галереи. Кроме того, троян может автоматически пересылать данный файл всем контактам в мессенджере.

🔑Конечная цель злоумышленников - получение доступа к платежным средствам, однако персональные данные и любая информация со смартфона также может быть использована в противоправных целях.

От кого бы вам ни пришло сообщение с неизвестным файлом, ни в коем случае не следует его открывать!

Обман с QR-кодами

В последнее время распространились способы обмана с QR-кодами, которые могут привести к финансовым потерям или передаче личных данных злоумышленникам.

QR-код из онлайн-банка

Мошенники научились красть деньги без данных банковских карт. Для этого им нужен только QR-код, который они выманивают у жертв по телефону.

В этой схеме используется сервис снятия наличных по QR-коду, доступный в некоторых банках. Клиент генерирует код на нужную сумму в мобильном приложении банка и подносит его к сканеру банкомата для получения денег.

Мошенники звонят жертвам под видом сотрудников банка и сообщают о «подозрительном» запросе на снятие денег. Чтобы его отменить, они просят прислать скриншот QR-кода. Ничего не подозревающая жертва отправляет код, с помощью которого злоумышленники снимают деньги из банкомата.

Социальные выплаты через Госуслуги

Распространенная мошенническая схема, связанная с размещением фейковых объявлений в общественных местах. Злоумышленники используют поддельные QR-коды, которые ведут на фишинговый сайт государственных услуг.

Жертва замечает объявление о гарантированной социальной выплате и переходит по ссылке на сайт, мимикрирующий под Госуслуги. Затем сканирует QR-код, который перенаправляет в чат-бот в популярном мессенджере. В чате человеку сообщают, что ему якобы положена выплата от государства.

В качестве жертв злоумышленники всегда выбирают социально незащищенную категорию граждан. Предлагают различные социальные выплаты и льготы, студенческие стипендии и пособия для семей с детьми. Под видом оформления положенных выплат аферисты обманным путем выманивают у людей личные данные и информацию о банковских счетах.

Замена QR-кода на поддельный

С помощью QR-кода можно удобно и быстро оплачивать покупки. Однако злоумышленники нашли способ обмануть и эту систему: они наклеивают поверх оригинального QR-кода свой поддельный код. Таким образом, мошенники получают деньги от ничего не подозревающих жертв. Злоумышленники используют поддельные коды для оплаты товаров, счета в кафе, а еще городского транспорта.

Недавно был выявлен новый вид мошенничества, связанный с арендой самокатов. Человек попытался арендовать самокат и привычно считал QR-код. Однако злоумышленники уже подменили код на собственный, а на смартфоне жертвы открылся совершенно другой ресурс. Человек непреднамеренно ввел свои личные данные и заполнил платежные формы, не подозревая о том, что они будут использованы мошенниками в корыстных целях.

Важно отметить, что использование поддельных QR-кодов поверх оригинальных обычно является разовой акцией мошенников. Однако всегда необходимо проявлять бдительность и перепроверять реквизиты, куда направляются средства по ссылке, открытой с помощью QR-кода.

Предложение вступить в домовой чат с использованием поддельного QR-кода.

В QR-код может быть интегрирована любая информация, например, ссылка на мошеннический сайт или на скачивание вредоносного программного обеспечения.

Чтобы защитить себя:

✅следует быть бдительным при просмотре электронных писем или сообщений;

✅никогда не предоставлять личные данные по непроверенным ссылкам;

✅не переходить по подозрительным веб-ссылкам;

✅не скачивать файлы из ненадежных источников;

✅использовать надежные антивирусные программы и программное обеспечение для защиты вашей информации.

Чтобы не стать жертвой мошенников, при взаимодействии с QR-кодами соблюдайте базовые правила цифровой гигиены:

Для оплаты рекомендуем использовать только динамические QR-коды, которые создаются специально для конкретной транзакции. Эти коды уникальны для каждого покупателя и отображаются на устройстве кассира. Считывая такой код, вы сможете проверить сумму платежа, реквизиты получателя и детали своего заказа.

При использовании бумажных QR-кодов следует проявлять особую осторожность. Прежде чем сканировать такой код, уточните у кассира или официанта, действителен ли он. Убедитесь, что код не наклеен поверх другого.

Фишинговые сайты часто используют незащищенное соединение или поддельные сертификаты безопасности. Перед тем как вводить свои платежные данные, важно убедиться в подлинности сайта и проверить наличие безопасного соединения — протокола HTTPS. Для этого посмотрите на адресную строку: если сайт использует безопасное соединение HTTPS, рядом с адресом будет значок замка.

Лучше не скачивать приложения на телефон с помощью QR-кодов. Злоумышленники могут использовать поддельные коды для распространения вредоносных программ. Если вы отсканируете такой код, то можете загрузить на свое устройство вирус или троянскую программу. <https://66.мвд.рф/news/item/59727870/>

Как распознать телефонного мошенника и не потерять свои деньги.

250 миллиардов рублей украли телефонные мошенники у российских граждан. 4 канал разработал инструкцию для доверчивых людей – обязательно изучите сами и поделитесь ей с вашими родственниками.

С каждым годом схемы обмана становятся всё изощрёнее. Чтобы убедить жертву, преступники разыгрывают «спектакли» и уверяют абонента, что он участвует в спецоперации государственной важности.

О популярных схемах преступного отъема денег у граждан и правилах безопасности – специальный репортаж Николая Палкина в рубрике #Безопасныйвзгляд. <https://vkvideo.ru/video-19179521_456249728>

Антирейтинг схем мошенников за 2024 год

Сотрудники управления по борьбе с киберпреступностью МВД России подготовили своеобразный антирейтинг схем мошенников за 2024 год.

Будут ли они и дальше использоваться для обмана граждан или останутся в уходящем году - зависит, в том числе, и от вас. Повышайте свою цифровую и финансовую грамотность, развивайте критическое мышление и, конечно, делитесь карточками рубрики #БезопасныйВзгляд с родными и близкими.

Еще в пресс-службе МВД рассказали о самых распространенных схемах получения мошенниками доступа к «Госуслугам» для хищения денежных средств <https://tass.ru/proisshestviya/22839071?ysclid=m5p1kltlds309053267> .

В первой злоумышленники звонят жертве, представляясь операторами связи, и просят код из сообщения под предлогом продления договора. На самом деле этот код дает доступ к личному кабинету «Госуслуг». Получив его, они меняют пароль и оставляют в подсказке номер телефона мошенников. Затем, позвонив по этому номеру, жертву убеждают, что через ее аккаунт кто-то пытается оформить кредиты и деньги нужно срочно перевести на «безопасный счет», чтобы их «спасти». **Защита – не брать трубку с незнакомых номеров, не говорить с мошенниками.**

Во второй схеме злоумышленники перевыпускают абонентский номер, который ранее использовался и теперь выставлен на продажу. После регистрации номера на себя они восстанавливают пароль к учетной записи «Госуслуг», привязанной к этому номеру, через одноразовый код. При этом законный владелец может не заметить взлом, так как доступ к приложению сохраняется. Получив доступ к «Госуслугам», мошенники оформляют онлайн-микрозаймы и кредиты, обращаясь в бюро кредитных историй, получая справки и регистрируя дополнительные номера с электронной подписью, сгенерированной через приложение «Госключ». **Защита – проверить свои старые неиспользуемые номера и удалить их со всех ресурсов, где ранее регистрировались (госуслуги, банки, магазины, аптеки, доставки и прочее).**

Также в 2025 году вместе с популяризацией искусственного интеллекта риски, связанные с ним, станут куда более явными. При помощи определенной программы злоумышленники могут буквально наложить изображение лица человека на любое фото или видео, взятое в интернете, и использовать это против жертвы в самых разных целях: от шантажа до опасной провокации. Еще злоумышленникам достаточно получить короткий образец голоса во время телефонного разговора или из перехваченного голосового сообщения, далее эту запись загружают в специальную программу, где всю работу уже делает нейросеть. С ее помощью можно совершить абсолютно любую манипуляцию.

Возможности легального приложения

<https://vk.com/video-228206245_456239042>

Наглядно демонстрируем как работает мошенническая схема, использующая возможности легального приложения NFCGate в сочетании с вредоносным программным обеспечением и социальной инженерией. NFC (коммуникация ближнего поля) технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров. Она используется при оплате покупок в магазинах или проезда в транспорте.

Принцип атаки заключается в перехвате NFC-трафика между банковской картой жертвы и NFC-терминалом банкомата. Устройство жертвы считывает NFC-данные банковской карты, а устройство злоумышленника принимает эти данные и эмулирует их непосредственно рядом с банкоматом.

Первый этап атаки чаще всего основывается на социальной инженерии, когда жертву под любым предлогом убеждают в необходимости установки специального приложения. Такое приложение внешне похоже на легитимное приложение банка или госструктуры, но на самом деле это вредоносная программа на основе NFCGate.

💬Как вариант, для удаленной установки NFCGate на устройство жертвы используют вредоносные RAT-приложения, однако это не отменяет необходимости поднести карту к смартфону.

🖥В устанавливаемом приложении уже указаны настройки сервера, на который будут отправляться NFC-данные при сканировании пользователем NFC-метки своим смартфоном. В этот момент на смартфоне злоумышленника уже запущена программа NFCGate в ожидании подключения к сессии смартфона жертвы.

❗️Обработанный таким образом сигнал позволяет получить доступ к счетам непосредственно через банкомат.

По данным экспертов (<https://www.facct.ru/blog/nfcgate/> ) в декабре 2024 и январе 2025 года зафиксировано не менее 400 атак на клиентов ведущих российских банков, средняя сумма списания составила около 100 тыс. рублей.

#Безопасныйвзгляд еще раз предупреждает, будьте бдительны! Не устанавливайте банковские и иные приложения из непроверенных источников и игнорируйте любые требования, связанные с прикладыванием банковской карты к смартфону для авторизации, подтверждения пароля или считывания данных.

Эксперты силовых ведомств Свердловской области рассказали о новых видах мошенничества и способах их избежать

👍Более 4 миллиардов рублей в 2024 году отдали уральцы телефонным мошенникам. Общая схема обмана давно известна: жертва отвечает на звонок с незнакомого телефонного номера, её запугивают, и она отдает преступникам все свои сбережения и имущество. Однако, доверчивость граждан продолжает оставаться распространенным явлением. Тем временем, мошенники изобретают новые способы, используя современные технологии, чтобы обмануть тех, кто не поддается их старым методам.

👍С помощью IT-технологий мошенники совершают треть своих преступлений: могут украсть личные данные, голос, взламывая аккаунты в соцсетях, создавая голосовые сообщения с помощью бота от нейросети.

❓Как пенсионер может лишиться двух собственных квартир? Что делать, если в мессенджере вы получили сообщение от якобы сотрудника ФСБ? И ещё, из совсем свежего: неожиданно вам пришел денежный перевод на небольшую сумму с очень странным сообщением… Как поступить? Как избежать обмана? В телесюжете ГТРК – рекомендации специалистов.

❗️И здесь, в заметке, напоминаем основные правила. Запомните сами и поделитесь с близкими:

- Нельзя самостоятельно возвращать «ошибочный» платеж от незнакомца, необходимо незамедлительно обратиться в банк.

- Не называйте звонящим коды из СМС.

- Сотрудники Центробанка никогда не звонят физическим лицам.

- Никаких «безопасных счетов» не существует.

- Настоящие сотрудники ФСБ никогда не рассылают сообщения, не требуют выслать данные онлайн. В случае необходимости они могут пригласить на официальную беседу по телефону или лично.

- Если есть подозрения, что сообщение в мессенджере – дипфейк, то нельзя загружать документы из сообщения или переходить по ссылкам.

- Перезвоните близкому, если от его имени к вам поступила просьба о срочной денежной помощи.

Куда обращаться в случае предложений о совершении преступления или угроз и психологического давления:

112 – единый телефон экстренной помощи;

88002227447 – горячая линия МВД России;

88007751717 – горячая линия психологической помощи МЧС России;

88002242222 – горячая линия ФСБ России.

Алгоритмы действий мошенников

«Скрипты» или алгоритмы действий мошенников могут быть очень разными, но почти все используют комбинацию психологических трюков. Эти трюки проверены практикой и научными методами и, в той или иной степени, работают:

❗️Срочность (эффект ограниченного времени)

Мошенники создают ощущение срочности: «Срочно подтвердите код, иначе ваш аккаунт заблокируют!». Срочность вредит способности человека к критическому мышлению. Человек действует эмоционально, а не разумно.

❗️Авторитет (эффект Милгрэма)

Мошенники представляются сотрудниками банка, полиции или ФСБ, потому что в природе большинства людей подчиняться авторитету. Уверенный, возможно, чуть-чуть грубоватый тон также способствует этому эффекту.

❗️Эмоциональное давление (страх или вина)

Вас пугают (например, «ваши родственники в беде») или пытаются вызвать чувство вины («из-за вашей ошибки система заблокирована»). Страх и вина также подавляют способность логически мыслить и приводят к подчинению.

❗️Иллюзия доверия (социальное доказательство)

Социальное доказательство — это психологический принцип, согласно которому люди выбирают, как им поступить, с оглядкой на поведение других людей. Мошенники говорят: «Все так делают», «Ваши друзья уже зарегистрировались».

❗️Комплименты и лестные отзывы

Мошенники могут хвалить вашу «проницательность» или упоминать некий «уникальный статус», чтобы получить расположение. Например, представившись сотрудником правоохранительных органов, могут попросить помочь выявить преступника. Жертва, попавшаяся на эту удочку, будет пытаться соответствовать статусу и завоевать доверие.

❗️Манипуляция недостатком знаний

Злоумышленник может использовать сложную терминологию, чтобы подтвердить свою экспертность, кроме того непонимание вызывает страх показаться некомпетентным, и человек соглашается на предложение.

❗️Ложная персонализация

Это маркетинговый прием, когда алгоритмы искусственного интеллекта пытаются создать иллюзию индивидуализированного опыта для пользователя, но на самом деле используют стандартные шаблоны и данные. Аферисты обратятся к вам по имени-отчеству, чтобы показать, что знают о вас все.

❗️Микрошаги к большой уступке (техника «нога в двери»)

Эффект приема «нога в двери» объясняют тем, что, оказав необременительную помощь при первой просьбе, индивид начинает осознавать себя отзывчивым человеком, готовым помочь другим в хорошем деле. Это повышает самооценку индивида, и человек бессознательно или осознанно налагает на себя моральные обязательства — быть таким же (нужным, отзывчивым) и впредь. Злоумышленники начинают с маленькой просьбы, например, «Назовите имя», а затем требуют большего.

Самое сложное - заметить, что вам пытаются манипулировать. Если понимать суть психологического трюка - сделать это будет намного проще.

✅Держите эмоции под контролем и не торопитесь с решениями.

✅Проверяйте информацию через официальный источник.

✅Не бойтесь отказывать или прерывать общение.

✅Повышайте финансовую и цифровую грамотность, чтобы распознавать уловки злоумышленников.

<https://t.me/cyberpolice_rus/2732>

1. **Рекомендации по защите**

Как обезопасить свои страницы

Как обезопасить свои страницы в социальных сетях и мессенджерах от взлома? 📵 Расскажем об этом в рубрике #Безопасныйвзгляд.

Множество разных компаний, больших и маленьких, незаметно или в открытую собирают информацию о нас, чтобы потом использовать её для своей выгоды или продать. Самый простой вариант - показать нам специально подобранную рекламу, на которую мы с высокой вероятностью кликнем.

На заре развития Интернета об этом никто не переживал. Но сейчас забота о личных данных становится такой же общественной нормой, как чистка зубов. С одной существенной разницей: если вы не почистили зубы вчера, вы можете сделать сегодня, а вот если ваши данные вчера утекли, то с этим уже ничего не поделаешь.

Производитель российского антивирусного программного обеспечения АО «Лаборатория Касперского» создал специальный сайт <https://privacy.kaspersky.com/ru/>, где собраны подробные инструкции о том, как подкрутить настройки приватности, чтобы личные данные оставались всегда под защитой. В одном месте собраны понятные описания настроек.

Проверьте свои устройства, которыми вы пользуетесь для общения «ВКонтакте», «Telegram», «WhatsApp» и другими.

Сделайте сами и поделитесь с близкими и знакомыми.

Правила финансовой безопасности

Уважаемые свердловчане, ГУ ВМД России по Свердловской области в рубрике #Безопасныйвзгляд знакомит с основным сводом правил финансовой безопасности <https://66.мвд.рф/news/item/59902847/> . Неукоснительно следуйте эти важным рекомендациям, чтобы не стать жертвой мошенников:

Правило 1.

В случае поступления звонков о том, что с Вашей банковской картой производятся несанкционированные операции либо на Ваше имя неизвестные пытаются оформить или оформили кредит (подали заявку на кредит), немедленно отключитесь от входящего звонка! Самостоятельно позвоните на «горячую линию» банка (звонок бесплатный), расскажите специалисту о ситуации, узнайте о состоянии Вашего счета.

Правило 2.

Никогда не сообщайте неизвестным людям по телефону какие- либо сведения о себе: в первую очередь, свои персональные данные, а также номера банковской карты (карт) – 16-значный номер на лицевой стороне карты и CVV-код, расположенный на ее обороте. Не стоит этого делать даже если позвонивший представился сотрудником банковской сферы, МВД, следователем, участковым уполномоченным, дознавателем, представителем прокуратуры, следственного комитета, ФСБ, юристом, адвокатом, и так далее. Не откровенничайте о себе или о своих родственниках. Помните важное правило – любой позвонивший, как бы он ни представился, – это неизвестное лицо!

Правило 3.

В случае, если позвонивший говорит о беде, случившейся с родственником (например, "он попал в ДТП"), и о необходимости передачи или перечисления денежных средств, незамедлительно положите трубку и, несмотря на то, что Вас просят никому ничего не говорить и никуда не обращаться, позвоните родственнику, о котором идет речь, а лучше, как можно большему количеству родственников, чтобы проверить полученную информацию. Можно позвонить в дежурную часть полиции (102, 902, 02), чтобы узнать, регистрировалось ли ДТП в указанном районе, и есть ли пострадавшие.

Правило 4.

Если у вас в семье есть дети, подростки, проведите с ними беседы об исключении фактов отклика на заманчивые предложения в интернете о быстром и легком заработке. Работа может быть связана с их участием в реализации мошеннических схем. Подобные деяния уголовно наказуемы вплоть до 10 лет лишения свободы.

Правило 5.

Не приобретайте по телефону никаких лекарств, путевок в оздоровительные и медицинские учреждения.

Правило 6.

При заказе в Интернете товаров сначала проверьте репутацию данного интернет-магазина, продавца (для этого введите ключевые слова – название магазина, ФИО продавца (если имеются), ассортимент предлагаемых товаров и др. — в разные браузеры («Гугл», «Яндекс» и так далее)).!!! Убедительная просьба - не ищите отзывы на странице сайта, где вы обнаружили заманчивую рекламу, ищите отзывы в разных браузерах. Только в случае обнаружения положительных отзывов решайтесь на приобретение. При этом не соглашайтесь на проведение оплаты по ссылкам, направляемым второй стороной сделки, как правило, они уводят на страницы мошенников. Требуйте от продавца доставки и оплаты за товар через почту наложенным платежом с дополнительной услугой «Опись вложения». В этом случае у Вас будет возможность до оплаты за посылку убедиться в ее содержимом, то есть в том, что направлен именно тот товар, который Вы заказывали. Если продавец не соглашается на такие условия, от товара лучше отказаться.

Правило 7.

Не старайтесь заработать в Интернете (в том числе на фондовых биржах, делая, так называемые, биржевые ставки, не старайтесь участвовать в инвестиционных программах - рекламу граждане находят во всплывающих окнах в интернете). Для осуществления такой деятельности необходимы опыт и специальные знания в области экономики, финансов, умения вести информационно-телекоммуникационный диалог в данной сфере деятельности. Указанный вид мошенничества, как правило, приносит гражданам многотысячные и миллионные финансовые потери!

Правило 8.

Не торопитесь перечислять денежные средства в ответ на сообщение, в котором содержится просьба о переводе денег, якобы, от знакомого вам человека, поступившее по телефону или в социальных сетях, на адрес электронной почты и так далее. Сначала самостоятельно свяжитесь с человеком, которому требуется помощь, чтобы убедиться, действительно ли это так.

Правило 9.

Не открывайте дверь незнакомым людям, даже если они представились работниками или сотрудниками государственных учреждений. Сначала позвоните в организацию и осведомитесь, работает ли такой сотрудник.

Правило 10.

Вас всегда должен насторожить визит человека, который предлагает обменять денежные средства, документы, что-то подарить или продать со скидкой и по льготной цене - это всегда обман. Любая адресная помощь от госучреждений оказывается только на бесплатной основе. А приобретение товаров с рук, не дает гарантии качества и, как правило, такой товар предлагается по завышенной цене.

Правило 11.

Не подписывайте никакие бумаги и документы, содержание которых вам непонятно (особенно, если это касается Вашей недвижимости, оказания каких- либо услуг). Ни под каким предлогом не отдавайте никому свои документы (паспорт, сберкнижку, документы на квартиру, иные). Во всех этих случаях посоветуйтесь со своими близкими и родными.

Правило 12.

Не заговаривайте с незнакомыми Вам людьми на улице, не откликайтесь на их предложения, какими бы выгодными и заманчивыми они ни были. Не рискуйте напрасно!

<https://66.мвд.рф/news/item/59902847/>

Рекомендации по настройке конфиденциальности и безопасности аккаунта Apple

🗣Продолжаем публиковать рекомендации по настройкам для обеспечения безопасности. Рекомендуется использовать следующие настройки для вашего Apple ID, чтобы защитить свои данные и снизить риск их утечки:

Войдите в учётную запись Apple с помощью браузера.

Вход и безопасность

Пароли для конкретных приложений: не сохраняйте пароли в заметках или браузерах. Используйте менеджеры паролей для надежного хранения и управления ими.

Персональные данные

Дата рождения: Не рекомендуем указывать достоверную информацию, чтобы затруднить злоумышленникам сбор ваших данных. Реальная дата рождения часто используется для восстановления аккаунтов.

Способы оплаты

Не сохраняйте платёжную информацию: Удалите данные банковских карт из аккаунта Apple. Это ограничивает использование мошенников в случае компрометации аккаунта. Храните платёжные данные в менеджере паролей для дополнительной безопасности.

Устройства

Удалите неиспользуемые устройства: В разделе «Устройства» проверьте, какие гаджеты подключены к вашему Apple ID. Удалите старые или неиспользуемые устройства, чтобы предотвратить доступ к данным на этом устройстве.

Конфиденциальность

Анализ данных iCloud: Отключите анализ данных iCloud. Это запрещает Apple использовать ваши данные для статистики и улучшения сервисов, сохраняя конфиденциальность.

Поступили средства от неизвестного отправителя

💵Если на вашу банковскую карту поступили средства от неизвестного отправителя, это может быть простой ошибкой. Но в отдельных ситуациях может быть началом мошеннической атаки.

❗️Рекомендуется предпринять следующие шаги:

1.Проверьте ваш счет: убедитесь, что деньги действительно зачислены на ваш счёт, проверив баланс через мобильное приложение или интернет-банк. Сообщение о зачислении средств может оказаться подделкой.

2.Свяжитесь с вашим банком: немедленно сообщите в ваш банк о неожиданном поступлении средств. Банк зарегистрирует ваше обращение и проведёт проверку.

3.Не тратьте полученные деньги: до выяснения обстоятельств не используйте поступившие средства. Расходование этих денег может быть расценено как необоснованное обогащение, что влечёт за собой обязательство возврата суммы и возможные судебные издержки.

4.Остерегайтесь самостоятельного возврата: если с вами свяжется отправитель с просьбой вернуть деньги на другие реквизиты, не соглашайтесь. Это может быть мошенническая схема (например, с последующим шантажом в связи с переводом «террористу» или транзитным переводом украденных денег через вашу карту). Все операции по возврату должны осуществляться через ваш банк.

5.Сохраняйте записи общения: Фиксируйте все контакты с предполагаемым отправителем, включая звонки и сообщения. Эти данные могут быть полезны в случае разбирательств.

✅Следуя этим рекомендациям, вы обезопасите себя от возможных мошеннических действий и правовых проблем.

1. **Меры государства**

Закон

Закон, направленный на защиту от кибермошенничества, принят Государственной Думой Федерального собрания Российской Федерации.

Он был поддержан депутатами единогласно 25.03.2025.

Вводится комплекс мер, пресекающих действия мошенников, среди которых:

1️⃣ Закрепление возможности онлайн-обмена информацией между государственными органами, банками и операторами связи.

2️⃣ При снятии денег через банкомат кредитная организация будет обязана осуществить проверку на наличие признаков выдачи средств без добровольного согласия.

В случае выявления этого банк должен на 48 часов ограничить выдачу наличных в сумме не более 50 тысяч рублей в сутки и незамедлительно уведомить клиента о причинах.

3️⃣ Предоставление гражданам возможности наделить родного или близкого человека статусом уполномоченного лица для получения подтверждения совершения операции по переводу денежных средств.

4️⃣ Обязательная маркировка звонков — на экране телефона оператор связи будет отображать наименование организации, откуда звонят, что позволит выявить мошенников.

5️⃣ Для сотрудников государственных органов, банков, операторов связи, маркетплейсов, сервисов по поиску работы и размещения объявлений устанавливается запрет на информирование граждан через мессенджеры.

6️⃣ Массовые вызовы и спам-звонки будут осуществляться только при условии получения предварительного согласия абонента, а при направлении отказа оператору связи — прекращены.

7️⃣ Предоставление людям возможности установить через Госуслуги или МФЦ самозапрет на заключение договоров об оказании услуг связи.

8️⃣ Введение запрета на передачу права пользования номером телефона третьим лицам, за исключением членов семьи.

Все эти меры позволят уберечь граждан от действий мошенников, а также будут способствовать сохранности их денежных средств.

Концепция государственной системы противодействия

Правительство России утвердило Концепцию государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий (<http://government.ru/docs/53922/>)

#Безопасныйвзгляд

💬Одной из важных частей государственной системы должна стать специализированная цифровая платформа, обеспечивающая оперативный обмен информацией между правоохранительными органами, Центральным банком, кредитными организациями и операторами связи для установления всех обстоятельств и лиц, причастных к мошенническим действиям.

Кроме того, документ предполагает принятие мер, направленных на:

✅Мониторинг информационных ресурсов и блокировку противоправного контента в сети Интернет.

✅Уточнение порядка предоставления цифровых услуг.

✅Оперативное приостановление операций с денежными средствами, используемыми в преступных схемах.

✅Развитие криминалистических методов и цифровых инструментов для расследования преступлений.

✅Участие в международных инициативах по борьбе с киберпреступностью.

✅Обучение специалистов и повышение их технической подготовки.

✅Информирование населения о рисках и методах защиты от цифровых преступлений.

Самозапрет на кредиты и займы

🙅‍♂️ На Госуслугах заработал сервис по самозапрету на кредиты и займы

Защитите себя от мошенников! Воспользуйтесь сервисом на Госуслугах, который позволяет установить добровольный запрет (https://www.gosuslugi.ru/644881/1/form) на выдачу кредитов и займов.

🟦 Как это работает

В кредитной истории тех, кто подал заявление, появляется специальная отметка с датой начала действия самозапрета. После этого банки и микрофинансовые организации должны отказывать в выдаче кредита или микрозайма. Наличие запрета можно проверить (<https://www.gosuslugi.ru/645081/1/form> ).

🟦 Что можно запретить

Запрет устанавливается на все потребительские кредиты и займы. При этом на Госуслугах можно по своему усмотрению ограничить выдачу полностью или частично. Например, можно запретить дистанционное оформление кредитов. В этом случае заключение договора будет возможно только при личном присутствии в офисе банка или микрофинансовой организации.

🟦 Ограничения

Возможность установить самозапрет не распространяется на ипотеку, образовательные и автокредиты, а также на уже заключённые договоры.

🟦 Как снять самозапрет

Снять ограничение (https://www.gosuslugi.ru/644941/1/form) можно в любой момент, подав заявление на Госуслугах. Понадобится электронная подпись. Создать её можно в приложении «Госключ». Так обеспечивается дополнительная защита от мошенников.

Самозапрет перестанет действовать на второй календарный день после внесения сведений в кредитную историю. Затем при необходимости можно установить новый запрет. Официальный аккаунт Минцифры России <https://t.me/mintsifry/2448>

Уральский форум «Кибербезопасность в финансах»

В преддверии Уральского форума «Кибербезопасность в финансах» <https://uralcyberfin.ru/> заместитель Председателя Банка России Герман Зубарев в интервью «Комсомольской правде» (<https://www.kp.ru/daily/27658/5047433/> рассказал о том, как будет работать период охлаждения при выдаче кредитов и займов, о новых требованиях ЦБ к банкам по открытию и обслуживанию счетов для несовершеннолетних и о первых результатах блокировки карт злоумышленникам.

«Мошенники меняют схемы регулярно, вариаций множество, и они зависят от типа потенциальной жертвы. Например, пенсионеров просят якобы подтвердить трудовой стаж, молодым предлагают заманчивое предложение о работе, кому-то присылают поддельные налоговые декларации. Обертка меняется, но главное для телефонных мошенников — получить код из смс или пуш-уведомления. Для этого они пугают и торопят, говорят, что вас только что хотели взломать, теперь нужно срочно защитить деньги. Долго кружат вокруг вас, якобы переключают между госуслугами, сотрудниками банка, Следственного комитета, других правоохранительных органов...Но в конце обязательно прозвучит, что надо спасти деньги и переправить их на какой-то безопасный или защищенный счет. Это главный сигнал опасности, своего рода «красная лампочка» тревоги, что нужно немедленно положить трубку. Мы постоянно говорим, но повторить не мешает: никаких безопасных счетов для «спасения» денег от мошенников в ЦБ не существует»

Центр правовой помощи гражданам в цифровой среде

Если вы стали жертвой онлайн-мошенничества или столкнулись с незаконной обработкой ваших персональных данных в интернете, обращайтесь за бесплатной юридической помощью:

💻 <https://4people.grfc.ru/>

✉️ 4people@grfc.ru

☎️ +74995508003

Центр правовой помощи гражданам в цифровой среде создан по инициативе Роскомнадзора Федеральным государственным унитарным предприятием «Главный радиочастотный центр» для оказания безвозмездной юридической помощи гражданам по защите прав и законных интересов в связи с обработкой их персональных данных в цифровой среде.

Центр сотрудничает с государственными органами, общественными объединениями и научными организациями. Осуществляется совместное оказание помощи гражданам, а также проводятся мероприятия, направленные на информирование о правилах безопасности в цифровой среде и способах защиты прав и законных интересов субъекта персональных данных.

Центр совместно с Многофункциональными центрами предоставления государственных услуг (МФЦ) активно развивает новые форматы оказания помощи населению. Именно в МФЦ обращаются граждане для восстановления доступа к учетной записи на портале «Госуслуги», а в Центр – за помощью в ликвидации юридических последствий действий мошенников.

Официальный телеграм-канал Главного радиочастотного центра (ФГУП «ГРЧЦ») <https://t.me/grfc_ru/446>

Методическое пособие

Совместной межведомственной рабочей группой в составе сотрудников правоохранительных органов, психологов, банковских структур под руководством ОМЦСП проделана работа по анализу способов профилактики мошенничествам в отношении граждан Свердловской области. Результатом стала публикация методического пособия «Психологические аспекты противодействия мошенничеству: как защитить себя и свою семью». В нем обобщены и систематизированы сведения о видах и способах мошеннических действий в отношении граждан. По каждому из них даны методы предотвращения и способы реагирования. Разобраны психологические способы действий злоумышленников, показана методика их противоправной деятельности. Определены технологические и психологические уязвимости каждого человека. Подробно освещены способы психологической защиты и техники саморегуляции эмоционального состояния. Постоянное нахождение в осознанности – залог защиты от манипулятивного воздействия.

Методический материал предназначен для изучения и использования в профилактической работе с сотрудниками и клиентами по данному направлению деятельности.

Ссылка для скачивания: <https://uralsocinform.ru/specialists/biblioteka-metodicheskikh-materialov/?SECTION_ID=334&ELEMENT_ID=2209>

1. **Обучающие мероприятия**

Минцифры России информирует, что ввиду участившихся случаев
интернет-мошенничества и телефонного мошенничества в рамках
информационного онлайн-проекта «Перезвони Сам» проводятся обучающие
семинары в очном и онлайн формате.
Главным приоритетом проекта является обеспечение граждан
и их близких актуальной информацией о возможных схемах мошенничества
в различных сферах жизнедеятельности и предоставление полезных инструментов противодействия таким ситуациям. Тематики вебинаров затрагивают широкий спектр проблем. Кроме того, слушатели могут задать вопрос экспертам вебинара.

1. «Мошенничество при покупке машины» - <https://vkvideo.ru/video-147412495_456239672>

2. «Как не стать жертвой мошенника? Разбираем истории обманутых
людей» - <https://vkvideo.ru/video-147412495_456239699>

3. «Безопасные покупки и продажи в интернете: как избежать мошенничества». Узнаем о популярных схемах обмана покупателей и продавцов в интернете, разберут реальные истории пострадавших, а также получат рекомендации, которые помогут защититься от действий злоумышленников. <https://vk.com/smartcityvdnh?z=video-147412495_456239744%2Fvideos-147412495%2Fpl_-147412495_-2>

Реальные истории из жизни, четкие инструкции и советы от экспертов
о том, как не стать жертвой мошенников в различных сферах жизни собраны
в одном месте — на сайте проекта <https://sam.mos.ru/>.

Анонс предстоящих мероприятий во 2 квартале 2025 года:

23 апр., 13:00

Продлите договор обслуживания сим-карты, или останетесь без связи. Схема мошенников под видом операторов связи

28 мая, 13:00

Только онлайн-трансляция

Мошенничество в онлайн-играх Мошенничество с внутриигровыми покупками: Как не стать жертвой

30 июн., 13:00

Только онлайн-трансляция

Мошенничество с использованием дипфейк-технологий: как не стать жертвой обмана?

Об основах личной информационной безопасности можно узнать на информационных ресурсах программы кибергигиены: <https://www.gosuslugi.ru/cybersecurity>.