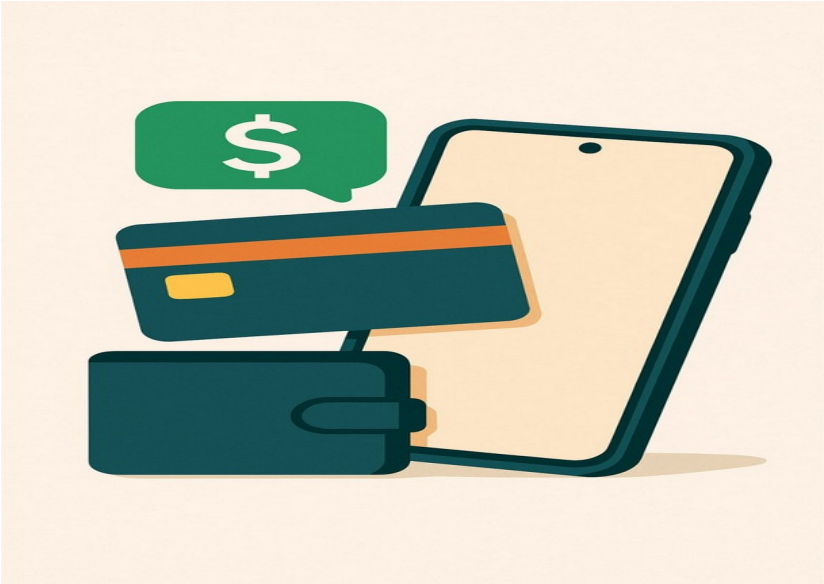


1 Неожиданный перевод на карту

Неожиданный перевод на карту может оказаться не подарком, а частью мошеннической схемы.

Злоумышленники могут использовать подобные переводы, чтобы добавить еще одно звено в цепь обналичивания средств или после получения обратного перевода начать запугивать гражданина под предлогом финансирования террористических организаций.

Если на вашу карту поступили средства от неизвестного отправителя, рекомендуется предпринять следующие шаги:

Проверьте поступление. Убедитесь, что деньги действительно зачислены на ваш счёт. Иногда мошенники рассылают поддельные уведомления о переводах. Проверяйте баланс только через официальный мобильный банк или сайт.

Сообщите в банк. Немедленно свяжитесь со своим банком — через горячую линию, чат в приложении или офис. Банк зарегистрирует обращение и проведёт проверку источника перевода.

Не используйте поступившие средства. Даже если сумма небольшая, её расходование может быть признано неосновательным обогащением, что влечёт обязанность вернуть деньги и возможные судебные издержки.

Не возвращайте перевод самостоятельно. Если кто-то сообщает, что «ошибочно перевёл деньги» и просит вернуть их на другие реквизиты, это может быть часть мошеннической схемы. Все операции по возврату должны проходить только через банк.

Используйте официальные функции возврата. В некоторых банках, например в Сбербанке, предусмотрена безопасная функция «возврата ошибочного перевода» прямо в приложении. Это исключает передачу данных посторонним и защищает от подделок.

Сохраняйте всю переписку и звонки. Зафиксируйте сообщения и контакты, связанные с переводом, — они могут пригодиться при разбирательстве.

Следуя этим рекомендациям, вы минимизируете риски и защитите себя.

2 Ошибки детей и их родителей в онлайн-среде

Самые частые ошибки детей и их родителей, облегчающие "работу" кибермошнников.

Дети:

Делятся личными данными, не осознавая, что аккаунт в социальной сети — это не просто информация, а ключ к их личности.

Верят в «лёгкие деньги» — выигрыши, бонусы, «донаты за репост». Так дети попадают в ловушки фейковых розыгрышей и игровых схем.

Общаются с незнакомцами, думая, что «в интернете все свои». Именно под видом новых друзей часто скрываются мошенники или вербовщики.

Скрывают свои аккаунты и публикуемый контент от родителей.

Боятся рассказать родителям о проблемах и затруднениях в сети.

Родители:

Не учат цифровой гигиене, считая, что ребёнок «и так всё знает». На деле дети умеют пользоваться гаджетами, но не умеют защищать себя.

Не устанавливают инструменты родительского контроля, хотя даже базовые фильтры блокируют до 70% подозрительных ссылок.

Пренебрегают безопасностью платежных средств - не ограничивают физический доступ к картам, сохраняют данные для доступа к приложениям, не ограничивают лимиты для детских карт.

Не следят за онлайн-покупками ребёнка, а между тем мошенники часто используют игровые платформы и маркетплейсы для мелких, но регулярных хищений.

Ругают детей за ошибки, вместо разъяснения способов защиты.

3 Безопасная онлайн среда для ребёнка

Количество несовершеннолетних, пострадавших от киберпреступлений за девять месяцев текущего года, возросло на 120%.

Это тревожный сигнал: мошенники "научились" похищать значительные средства, воздействуя на детей. В ход идет полный арсенал схем и психологических манипуляций, адаптированных под возрастную группу. Обеспечение цифровой безопасности детей становится задачей не только для специалистов, но и для каждой семьи.

Интернет даёт знания, друзей и хобби, но и открывает дверь для мошенников, агрессии и фейков.

Как создать безопасную онлайн-среду для ребёнка — шесть простых шагов:

Начать с доверия.

Главный фильтр — не приложения, а общение. Если ребёнок знает, что может рассказать родителям о странных сообщениях, угрозах или просьбах «отправить фото», вы уже обеспечили половину защиты.

Онлайн вместе.

Совместные просмотры фильмов, участие в играх и обсуждение блогеров помогают родителям оставаться в курсе интересов ребёнка и мягко объяснять, где безопасно, а где — манипуляция.

Правила — это не запрет, а рамки безопасности.

Договоритесь о времени в сети и зонах, где устройства не используются. Пусть ребёнок сам участвует в определении этих границ — тогда контроль воспринимается как забота, а не наказание.

Родительский контроль — ваш цифровой помощник.

Настройки в смартфоне, браузере и операционной системе позволяют ограничить нежелательный контент, видеть установленные приложения и время использования. Главное — объяснить ребёнку, зачем это нужно.

Мини-курс по киберграмотности.

Научите ребёнка не переходить по подозрительным ссылкам, не сообщать личные данные, пароли и одноразовые коды. Объясните, что даже «игровые бонусы» или «подарки» могут оказаться ловушкой мошенников.

Контроль финансов и микроплатежей.

Если ребёнок делает онлайн-покупки, оформите отдельную карту с ограниченным лимитом. Так проще контролировать расходы и избежать неожиданных списаний.

Главное правило: в цифровом мире нет стопроцентной защиты, но есть осознанность, внимание и диалог.

Безопасность ребёнка в интернете начинается не с блокировки сайтов, а с доверия — и вашего участия в его онлайн-жизни.

4 Как уберечь персональные данные при продаже смартфона

Смартфоны хранят много личных данных — перед продажей или передачей их нужно надёжно удалить. Подготовили для вас инструкцию по "предпродажной" подготовке Android и iOS для обеспечения максимальной безопасности ваших данных.

Очистка Android:

Шаг 1. Включите шифрование (если оно не включено)

Современные Android-устройства шифруют данные по умолчанию; на старых моделях шифрование может быть отключено, что позволяет восстановить удалённые данные.

Проверяйте состояние шифрования в разделе «Настройки» → «Безопасность» → «Шифрование». Если эта функция неактивна, включите её и дождитесь окончания процесса.

Шаг 2. Удалите все аккаунты

Ваш смартфон может содержать важные учетные записи, включая Google-аккаунт и специальные профили производителей вроде Samsung, Huawei, Xiaomi и других. Оставленные учетные записи могут заблокировать активацию устройства новым владельцем.

Зайдите в меню «Аккаунты» в настройках системы и последовательно удалите каждую учётную запись вручную.

Шаг 3. Сделайте полный сброс к заводским настройкам

Для полной очистки рекомендуется выполнить сброс к заводским параметрам:

Откройте «Настройки» → «Система» → «Сброс» и выберите пункт «Удаление всех данных (сброс к заводским настройкам)». Процесс займет некоторое время, после чего устройство перезагрузится.

Шаг 4. Заполните свободное пространство файлами

После сброса, не настраивая телефон, включите камеру и запишите длинные видео до заполнения памяти — это перезапишет остаточные данные. Затем выполните сброс ещё раз. Этот трюк перезапишет свободные блоки памяти, где могли остаться ваши данные, сделав их восстановление практически невозможным.

Очистка iPhone (iOS)

Несмотря на то, что Apple уделяет большое внимание вопросам конфиденциальности, полная подготовка устройства требует внимательного подхода.

Шаг 1. Отключите «Найти iPhone» и выйдите из iCloud

Эти шаги особенно важны, поскольку без отключения функций защиты ваше устройство не удастся активировать новым пользователям.

Перейдите в «Настройки» → [ваше имя] и внизу страницы нажмите «Выйти». Подтвердите выход, введя пароль своего Apple ID.

Также убедитесь, что отключён сервис «Найти iPhone».

Шаг 2. Удалите весь контент

Используйте встроенную функцию стирания содержимого и настроек:

«Настройки» → «Основные» → «Передача или сброс iPhone» → «Стереть контент и настройки»

После подтверждения все личные данные и зашифрованные ключи будут удалены, а устройство вернётся к состоянию нового гаджета.

Шаг 3. Убедитесь, что устройство не привязано

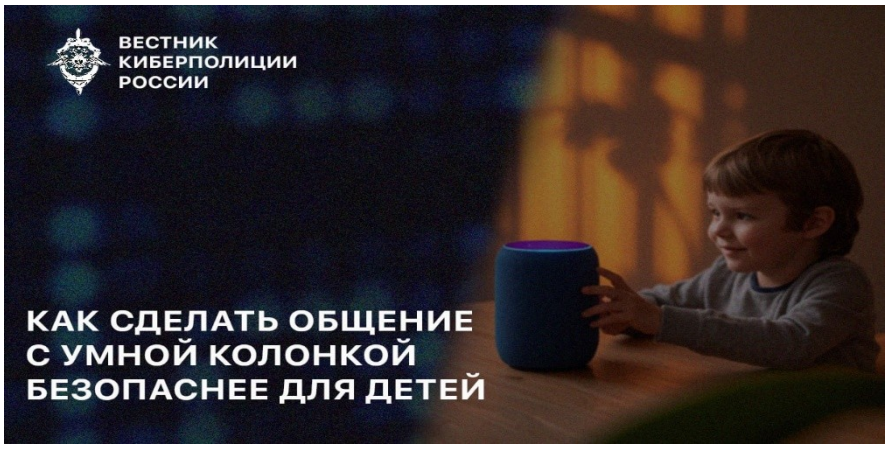
После сброса проверьте экран приветствия. Если появится начальное окно активации — значит, очистка прошла успешно.

Не подключайтесь повторно к устройству!

Дополнительные советы:

➡️ SIM-карту лучше извлечь и хранить отдельно либо утилизировать безопасным способом.

➡️ SD-карты требуют отдельного внимания: отформатируйте их перед передачей или оставьте себе.



5 Безопасное общение с умной колонкой

Напомним, что в начале этого года ВЦИОМ совместно с Альянсом по защите детей в цифровой среде провёл опрос родителей детей до 14 лет. Согласно его результатам, 91% родителей разрешают своим детям пользоваться «умной» колонкой как минимум раз в неделю, из них 54% — ежедневно, а 33% — несколько раз в неделю.

Учитывая высокую вовлечённость детей в использование голосовых помощников, важно понимать потенциальные риски и знать меры защиты.

Защита конфиденциальности при сборе данных.

Компании собирают данные о предпочтениях (любимая музыка, вопросы, которые вы или ваш ребенок задаете, интересы). Это используется для таргетированной рекламы и создания профиля пользователя.

Решение - Отключите персонализированные ответы.

Это не даст колонке использовать историю поисков и запросов для формирования ответов, что повышает конфиденциальность.

В приложении: —> Перейти в настройки: нажать «→ ». —>Отключить опцию «Персонализированное общение».

Чтобы очистить контекст, нажать «Удалить контекст» и подтвердить удаление.

Неподходящий по возрасту контент: Музыка с ненормативной лексикой, подкасты или новости на тревожные темы, ответы на вопросы, которые ребенок не готов воспринимать.

— Обязательно включите «Детский режим».

— Убедитесь, что активированы фильтры контента и безопасный поиск.

— Проверьте, какие навыки/действия разрешены: отключите всё стороннее, кроме проверенных.

→ Настройки профиля → «Детский режим» → выбрать возраст ребёнка → включить фильтрацию.

Голосовые покупки и управление «умным домом»

Ребёнок может случайно оформить заказ или включить опасные устройства (замки, электроприборы).

— Отключите голосовые покупки в настройках аккаунта.

— В «умном доме» запретите колонке управлять критичными устройствами через настройки в приложении.

Также через приложение можно настроить оповещения о попытках доступа к запрещённому контенту, продолжительности использования устройства и других значимых событиях.

Ниже - общие рекомендации по настройкам безопасности умных устройств:

Правильно настройте домашнюю Wi-Fi сеть: используйте надёжный пароль и надёжное шифрование.

Сразу после настройки устройства измените его имя — чтобы киберпреступникам было сложнее определить модель.

Измените установленный по умолчанию пароль. Создайте надёжный пароль и регулярно его меняйте. Не используйте одинаковые пароли на разных устройствах.

Если есть возможность, используйте многофакторную аутентификацию для доступа к устройству.

Вовремя устанавливайте обновления программного обеспечения вашего устройства.

Внимательно прочитайте политику конфиденциальности, особенно в отношении использования личных данных.

Проверьте в настройках параметры конфиденциальности, отключите те разрешения, которые считаете лишними.

Научите детей обращаться к вам в случае, если колонка сказала что-то странное или пугающее и обязательно рассказывайте детям о правилах цифровой гигиены, дайте понять, что колонка — машина, а не человек

6 Принцип нулевого доверия

Минимум, который работает

Мы часто повторяли, что принцип нулевого доверия — лучшая защита. Не выполнять никаких требований, пока не будет доказана их легитимность, не переходить по ссылкам, не открывать вложения, не доверять даже знакомым, пока не проверишь.

Но у этой системы есть один очевидный недостаток — ограниченность человеческих ресурсов. Наше внимание можно перегрузить, если проверять каждое сообщение, сверять адреса сайтов, перезванивать по номерам с официального сайта после каждого письма. Это неприятный факт, но абсолютно реалистичный.

И киберпреступники это прекрасно понимают. Они не взламывают системы — они взламывают внимание. Любая усталость, спешка, переключение между задачами работает на них. Поэтому важно не стремиться к идеальному «нулевому доверию», а выстроить минимальный, но устойчивый уровень защиты, который реально выдержит повседневный ритм.

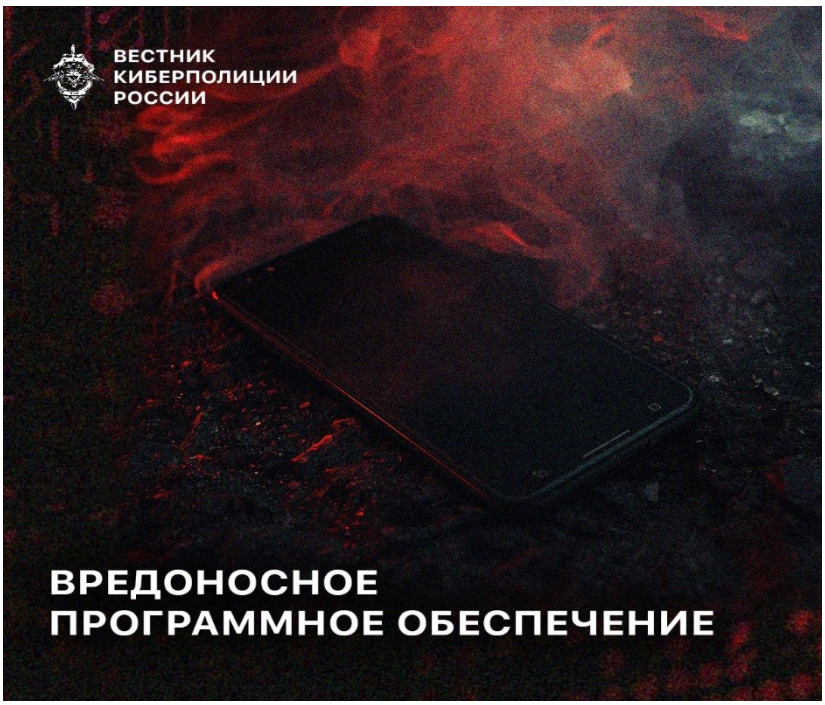
Три базовых привычки:

➡️Не действовать с ходу. Любая просьба «срочно», «прямо сейчас» — сигнал стоп. Даже 10 секунд паузы позволяют мозгу вернуть контроль.

➡️Один канал доверия. Выберите единственный способ для критичных действий — например, только личный звонок по известному номеру. Все остальные каналы («новый чат», «альтернативный аккаунт», «резервная ссылка») автоматически под подозрением.

➡️Три тревожных маркера. Срочность, эмоции, риск упустить выгоду, персональные данные. Если в сообщении есть хотя бы два — перед вами, скорее всего, фишинг или социальная инженерия.

Никакая система не даст полной гарантии. Но эти простые правила экономят главное — внимание. Именно оно остаётся последней линией обороны между человеком и злоумышленниками в сети Интернет.



7 Вредоносное программное обеспечение

Ранее мы уже рассказывали о распространённых вредоносных программах, активно используемых в мошеннических схемах в России: банковском трояне Mamont, модификации NFCGate и RAT-утилите CraxsRAT.

Арсенал киберпреступников постоянно пополняется - нами зафиксирован рост активности шпионских программ LunaSpy и SpyNote.

LunaSpy — программа шпион, распространяется через мессенджеры под видом антивируса и программ банковских защитников.

Функции:

Имитирует сканирование и показывает фальшивые угрозы.

Перехватывает сохранённые пароли из браузеров, записывает экран, крадёт галерею.

Записывает звук и видео с микрофона и камеры.

Читает SMS, журнал звонков и список контактов.

Запускает произвольные shell-команды.

Отслеживает геолокацию.

Записывает экран.

SpyNote — RAT (троян удалённого доступа). Используется телефонными мошенниками после «разговора поддержки» с просьбой установить «спецпрограмму для защиты».

Функции:

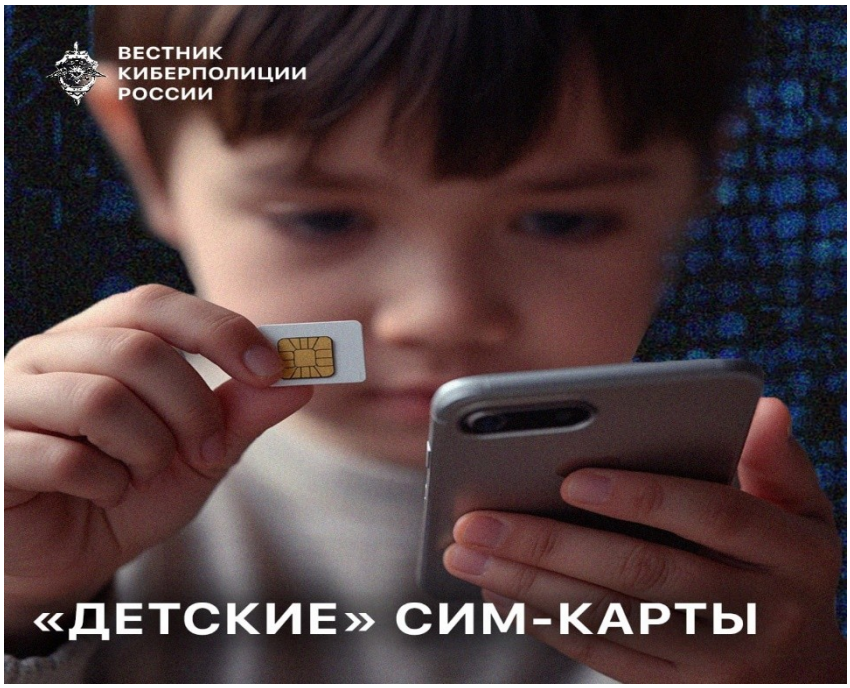
Полный удалённый контроль над устройством,

Перехват SMS и уведомлений,

Overlay-атаки на банковские приложения.

Цель - получение доступа к онлайн-банкингу и мессенджерам.

Чтобы избежать заражения шпионскими программами вроде LunaSpy и SpyNote, устанавливайте приложения только из официальных магазинов, регулярно обновляйте систему и программы, ограничивайте права приложений и пользуйтесь надежными антивирусами. Не переходите по подозрительным ссылкам и файлам из мессенджеров, включите двухфакторную аутентификацию и будьте внимательны к рекламным баннерам и всплывающим окнам. Следование этим мерам существенно повысит вашу защиту.



8 Детские сим-карты

«Детские» SIM-карты: защита от мошенников и новые возможности для родителей

В России планируется запуск специальных «детских» SIM-карт — инициатива направлена на усиление защиты несовершеннолетних от киберугроз и телефонных мошенничеств. С предложением выступил заместитель председателя Совета по развитию цифровой экономики при Совете Федерации Артём Шейкин, а реализацию меры подтвердил Министр цифрового развития, связи и массовых коммуникаций Максут Шадаев.

Основные особенности нововведения:

Телефон ребёнка сможет взаимодействовать только с заранее проверенными контактами и сайтами;

При поступлении подозрительного звонка или попытке мошенничества система будет мгновенно уведомлять родителей;

Родители получат возможность отслеживать местоположение ребёнка в режиме реального времени без необходимости подавать официальное заявление или получать судебное решение.

«Чтобы защитить детей от мошенников и киберрисков, необходимо идти дальше технических фильтров», — подчеркнул Артём Шейкин.

Помимо этого, аналогичный подход будет применён и к другой уязвимой категории граждан. Пожилые пользователи смогут назначить доверенное лицо через портал «Госуслуги», которому будет предоставлен доступ к их геоданным — например, для помощи в экстренных ситуациях.

➡️Инициатива отражает общенациональный курс на цифровую безопасность и защиту тех, кто наиболее подвержен рискам в онлайн- и телефонном пространстве. Реализация проекта будет сопровождаться работой с операторами связи и разработчиками сервисов, чтобы обеспечить как эффективность, так и соблюдение прав пользователей.

9 Поведение ребёнка в сети

О чём может говорить поведение ребёнка в сети

Дети доверчивы. Этим злоупотребляют люди, которые используют несовершеннолетних в корыстных целях. Иногда они могут заставить ребёнка навредить себе или присоединиться к экстремистскому движению.

Обратите внимание, если в соцсетях ребёнка:

Посты или изображения с признаками увечий (порезы, синяки, кровь);

Контент с депрессивной, суицидальной или нигилистической тематикой;

Увлечение фигурами, связанными с насилием;

Цитаты, обесценивающие жизнь или традиционные ценности.

Что должно насторожить в поведении ребёнка:

Ребёнок стал скрытным: не рассказывает, где был, с кем общается;

Избегает представления новых «друзей» и не даёт их контакты — особенно онлайн-знакомых;

Резко ухудшились школьные результаты или пропал интерес к учёбе;

Пользуется дорогими вещами, которых вы ему не покупали;

Распоряжается личными деньгами, полученными не от родственников.

Эти признаки не всегда означают вовлечение в деструктивную среду — но они могут быть сигналом, что ребёнку нужна помощь. Главное — не запрет и принудительная проверка телефона, а доверительный диалог и готовность выслушать.

Если вы видите угрозу, но ребенок не идет на контакт - обратитесь к школьному психологу, в подразделение по делам несовершеннолетних или на горячую линию консультативной помощи подросткам и их родителям в сети Интернет (телефон 8-800-200-01-22).

10 Смена сим-карты

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?

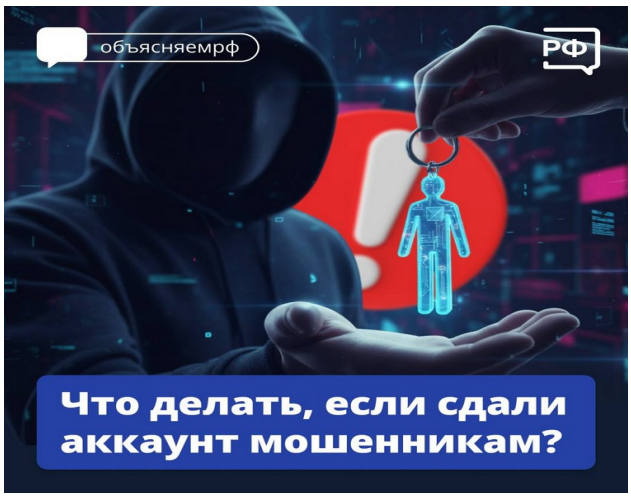
Первым делом открепите неиспользуемый номер телефона от портала «Госуслуг», онлайн-банка и других своих аккаунтов.

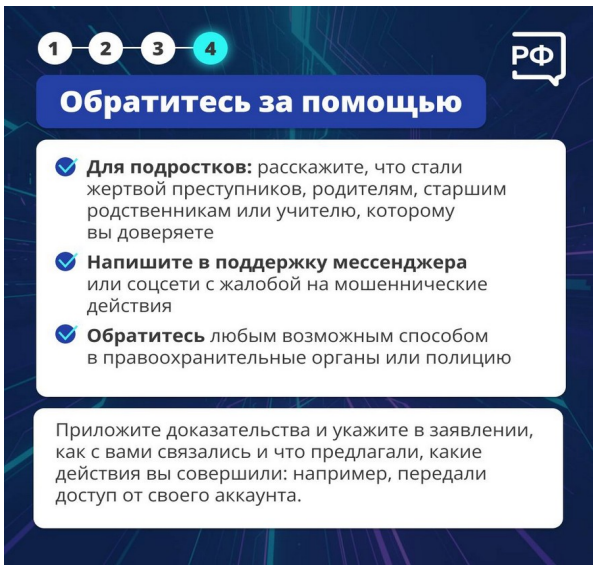
Сделать это самостоятельно можно, если сим-карта, которой вы не планируете больше пользоваться, все еще установлена в вашем телефоне. Связано это с тем, что на этот номер придет код, подтверждающий ваши действия.

Сменить номер телефона достаточно просто, на портале «Госуслуги» нужно перейти в раздел «Настройки и безопасность» 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.

Будьте бдительны и предупредите родных и близких!





11 Ответственность за сдачу аккаунтов в соц сетях

Давать аккаунт в соцсети или мессенджере в аренду — плохая идея.

Так вместо лёгкого заработка вы можете получить штраф от 30 тыс. до 50 тыс. рублей или даже стать фигурантом уголовного дела. Почти всегда «арендатор» оказывается мошенником, а вы — его сообщником.

Если вы поняли, что влипли, действуйте по инструкции, которую мы подготовили в нашей новой рубрике вместе с Киберполицией России. Это поможет избежать уголовной ответственности, свести к минимуму риск административной, ведь вы докажете, что не хотели нарушать закон, а наоборот — остановили преступление.

На юридическом языке это называется «добровольный отказ от преступления» или «добровольное прекращение противоправного поведения», и оба этих обстоятельства всегда учитываются.

Кроме того, если вам меньше 16 лет, следование нашей инструкции поможет спасти от административной ответственности ваших родителей.

12 Мошенничество в компьютерных играх

В текущем году в компьютерных играх зафиксировано порядка 1000 фактов мошенничества. В нашем антирейтинге и в глобальном рейтинге мобильных игр по загрузкам лидирует Roblox.

Рассказываем о самых распространенных схемах мошенничества на этой площадке:

▶Злоумышленники чаще всего действуют через яркие видео, «ограниченные» предложения или фейковые раздачи, в игровых чатах, Discord-серверах, соцсетях или пишут ребёнку прямо в игре — под видом «подарка», «конкурса» или «выгодной сделки».

«Одноразовый» Game Pass

Мошенники продают Game Pass, обещая особые функции или преимущества. На деле такие пропуска либо не дают ничего сверх обычного, либо работают только до перезапуска игры — после выхода из сессии они исчезают, и за них приходится платить снова.

«Невидимая» одежда

Рекламируются и продаются скины, которые якобы делают персонажа невидимым. В реальности это просто прозрачные предметы, которые выглядят как белая рубашка или пустота — никакой спецэффект не работает.

Мини-игры-ловушки

Например, появляется окно с надписью: «Сколько раз ты можешь кликнуть за минуту?». После активного нажатия игроку предлагают купить дорогой предмет, Game Pass или подписку — якобы за «рекорд». На самом деле это просто способ навязать покупку.

Поддельные «испытания на Robux»

В таких локациях ребёнка окружают боты или фейковые игроки, которые кричат: «Получил Robux!», «Это работает!», «Пройди испытание!». В конце просят ввести логин и пароль от аккаунта. Никогда не передавайте эти данные — это приведёт к краже аккаунта и, возможно, привязанных платёжных средств.

Фишинговые ссылки

Мошенники отправлять ссылки «для получения бесплатных Robux». Такие сайты имитируют Roblox, просят логин и пароль или данные карты, а затем блокируют аккаунт и списывают деньги.

Покупка Robux вне официального магазина

Предлагают «выгодно» купить валюту по заниженной цене — но только за пределами платформы. Чтобы «оплатить», просят данные родительской карты. Деньги списывают, а Robux не появляются. В худшем случае — получают доступ к карте и продолжают списания.

«Ты выиграл! Получи приз»

Ребёнку сообщают, что он выиграл Robux в «конкурсе», но для получения нужно ввести данные аккаунта. После этого мошенник меняет пароль и получает полный контроль над профилем — включая историю покупок и привязанные платёжные методы.

Ребёнок не глуп, если поверил — просто ему не с чем сравнивать. Поэтому лучше заранее объяснить, на что стоит обращать внимание. А ещё надёжнее, договориться, что любые покупки, регистрации, привязка почты или переход по внешним ссылкам должны происходить вместе с родителями или под их контролем.

13 Актёрский состав мошенников

Актёрский состав одного телефонного звонка

▶Современная мошенническая схема часто напоминает сериал с низким бюджетом, где сценарий строго «по учебнику», а один и тот же актер играет сразу несколько ролей.

Ниже набор образов из одного эпизода (к сожалению, не сериала, а уголовного дела):

«Добрый бухгалтер из администрации»

Первая сцена. Спокойный, вежливый голос сообщает о «выплате» или «проверке документов». Главная задача — первый контакт и выманивание кода авторизации.

«Специалист техподдержки портала Госуслуги»

«Технический специалист» сообщает о якобы взломе аккаунта, «подозрительных действиях» или «угрозе утечки данных». Именно эта роль создаёт первую тревожную сцену и формирует ощущение, что ситуация требует немедленных действий.

«Суровый майор»

После появления «специалиста» на сцену выходит представитель силового блока. Использует юридическую лексику, говорит о «подозрительных финансовых операциях», «угрозе ответственности» и давит на эмоции.

«Столичный юрист-спаситель»

Создаёт иллюзию легитимности. Предлагает «законную схему защиты» и называет адрес офиса для солидности.

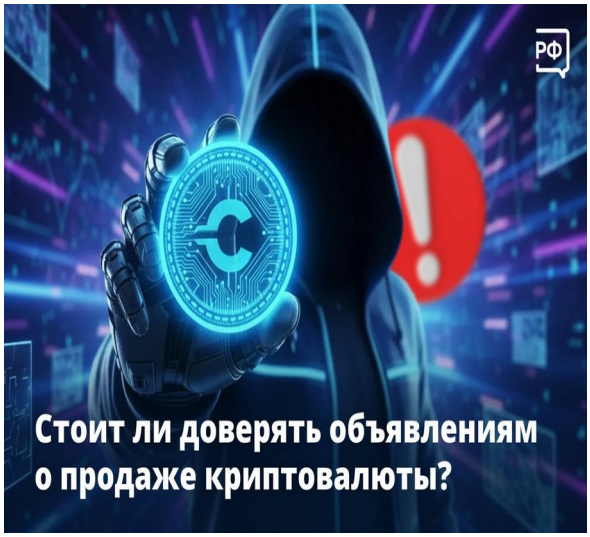
«Сотрудник по контролю и надзору за финансовым мошенничеством»

Кульминация. Заявляет, что на имя гражданина открыты счета, идут переводы, а единственный способ «защитить средства» — выполнить ряд срочных указаний, включая выдачу наличных или перевод средств.

«Курьер в костюме»

Финальный исполнитель — человек, которому передаются деньги. Молча получает пакет, называет пароль и исчезает.

Мораль проста: если вам по одному сценарию звонят пять разных людей — вы не в сериале «Клан Сопрано», вы в эпицентре мошеннической схемы.



14 Объявление о продаже криптовалюты

«Купите криптовалюту на сумму от 500 рублей, перепродайте и получите 150 тыс. рублей стабильного дохода в месяц» — такие объявления нередко можно встретить в мессенджерах. Не спешите верить: лёгкие деньги обещают только мошенники. Почему — рассказываем в специальной рубрике Объясняем.рф и Киберполиции России.

Даже если вас не обманут напрямую, стабильного дохода вы точно не получите. Мошенники никогда не говорят о скрытых рисках — например, об ограничениях вывода средств и нормативных препятствиях.

Важно! Более трети всех блокируемых мошеннических ресурсов предлагают инвестиции в криптовалюты. Главные признаки таких афер:

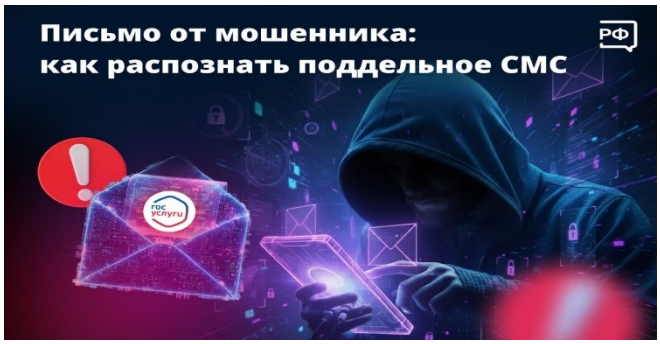
— гарантия прибыли без рисков;

— много непонятной графики и статистики;

— отзывы «успешных» инвесторов;

— вас склоняют к быстрому решению;

— отсутствие юридической информации (нет номера лицензии, сведений о договоре).



15 Как распознать поддельное СМС

Пришло СМС от Госуслуг? Вам запросто могут писать мошенники. Аферисты часто отправляют людям сообщения якобы от официального портала, чтобы жертвы сами звонили им и передавали личные данные. В специальной рубрике Объясняем.рф и Киберполиции России рассказываем, как определить фейк.

▶Неправильный номер

Настоящие сообщения от Госуслуг приходят только с короткого номера 0919 или буквенно-цифрового ID gosuslugi.

▶Сообщение пришло в мессенджер

Официальные службы не пишут людям в WhatsApp*, Telegram или другие мессенджеры.

▶Вас просят перезвонить в «техподдержку»

У Госуслуг два официальных номера: 8 (800) 100-70-10 и 115. Если вас призывают позвонить по другому номеру, это мошенники.

▶В сообщении есть подозрительная ссылка

Госуслуги никогда не присылают пользователям ссылки для входа или подтверждения данных.

▶Вас торопят и пугают

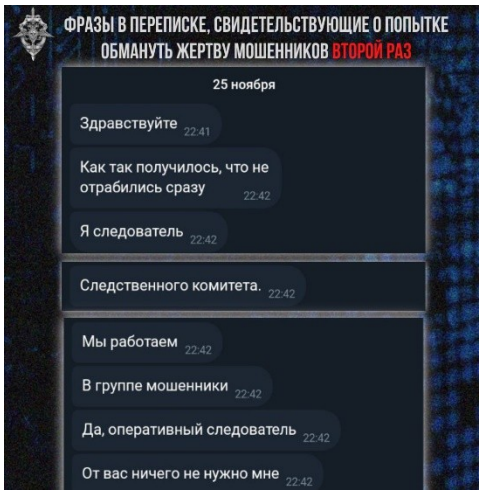
Сообщения о «взломе» или «подозрительной активности» — психологический приём, который мошенники используют для давления на человека.

▶В тексте есть ошибки

Официальные сообщения от государственных служб тщательно проверяют. Орфографические и пунктуационные ошибки — признак подделки.

Не звоните по номерам и не переходите по ссылкам из СМС. Заблокируйте отправителя и сообщите о подозрительной рассылке через обратную связь на сайте, по горячей линии 8 (800) 100-70-10 или в полицию (если пострадали).

* Продукт компании Meta, признанной экстремистской и запрещённой на территории России.



16 Повторный обман

Повторный обман жертв мошенничества: как работает «вторая волна»

После столкновения с мошенниками человек нередко ищет способ «вернуть деньги» или хотя бы понять, что делать дальше. И именно в этот момент риск повторного обмана становится максимальным. В анонимных Telegram-каналах сформировалась целая экосистема персонажей, которые работают исключительно на уязвленное состояние пострадавших. Формально они предлагают помощь, но фактически создают условия для нового преступления.

Кого там можно встретить:

➡«Юристы», которые не имеют ни лицензии, ни офиса, ни документов. Они уверяют, что знают «особые лазейки» и могут «вернуть средства», а затем вымогают деньги за фиктивные консультации, платные обращения и «подачу ходатайств», которые никто никогда не увидит.

➡«Хакеры широкого профиля».

По легенде — способны «отследить деньги», «заблокировать карту злоумышленника» или «вернуть перевод». В реальности — обычные мошенники, которые используют техническую терминологию и продают воздух.

➡«Оперативные следователи».

Они якобы «ищут потерпевших» или «работают в госпрограмме». Такие персонажи играют на доверии к силовым структурам и выкачивают деньги под предлогом «помощи следствию».

➡️«Решалы», якобы когда-то работавшие в мошеннических кол-центрах. Пользуясь эмоциональным состоянием жертвы, предлагают «решить вопрос через людей с той стороны».

Почему пострадавшие попадаются повторно?

Человек пережил шок, хочет восстановить контроль над ситуацией и готов верить любому, кто обещает быстрый результат. Именно на этом строится «вторая волна» мошенничества.

Единственный безопасный алгоритм после мошенничества: заявление в полицию, обращение в банк, в прокуратуру, работа с проверенными государственными сервисами и юридическими структурами.

17 Мошенники на маркетплейсах

Инструкция по разоблачению мошенников с маркетплейсов

▶Схемы мошенничества на популярных китайских маркетплейсах становятся всё изощрённее: фейковые трекномера, нейросетевые отзывы, «зеркала» известных магазинов и скрытые доплаты при оформлении заказа. Но защититься можно - если знать правила игры.

Проверяйте трек-номер не только на маркетплейсе, но и через независимые сервисы: Почта России (https://www.pochta.ru/), Cainiao (https://cainiao.ru/) и др. Если статус «завис» или расходится с данными - это тревожный сигнал.

Анализируйте отзывы: новые аккаунты, однотипные фото, идеальные ракурсы — признаки накрутки. Ищите негатив и проверяйте изображения через поиск по картинкам.

Читайте описание до конца - нём часто скрывают реальную комплектацию или статус «реплики».

Сверяйте название и URL магазина. Одна лишняя буква - и вы в поддельном «официальном» магазине.

Общайтесь с продавцом до оплаты. Уклончивые ответы или отсутствие реакции — повод отказаться от покупки.

Не соглашайтесь на доплаты. Отменяйте заказ, пока статус «ожидает отправки».

При проблеме — открывайте спор: приложите фото, видео распаковки, скриншоты описания и чата. Чем больше доказательств — тем выше шанс на полный возврат.

Маркетплейсы стараются защищать покупателей, но только если вы сами проявляете бдительность.

Не спешите нажимать «купить» и всегда проверяйте детали.

18 Через Apple ID

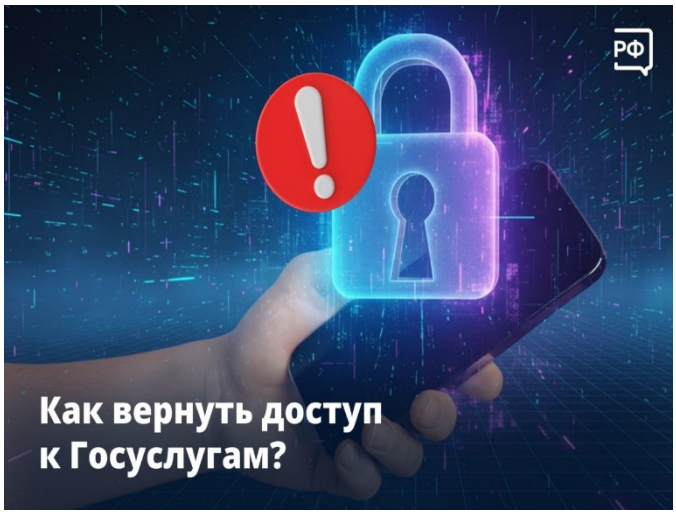
Новый способ мошенничества с Apple ID, активно реализуемый через «получение доступа к играм».

Злоумышленники, маскируясь под продавцов цифрового контента, предлагают пользователям временно авторизоваться в стороннем аккаунте Apple ID под предлогом установки игровых приложений. Их мотивация звучит убедительно, ведь требуется «активировать недоступный контент», «разблокировать премиальную версию» или получить «доступ по сниженной цене».

➡️ Как только пользователь вводит чужие логин и пароль от Apple ID на своём устройстве, злоумышленники активируют функцию «Найти iPhone» и переводят устройство в режим «Потерян», тем самым полностью блокируя его.

Пользователю приходит сообщение с требованием перевести деньги за разблокировку, часто сопровождаемое угрозами удаления данных или распространения личной информации.

Следует помнить, что вход в чужой Apple ID на своем устройстве даёт злоумышленнику полный контроль через iCloud.



19 Как вернуть доступ к Госуслугам

Мошенники получили доступ к вашему аккаунту на Госуслугах? Важно действовать быстро, чтобы аферисты не успели взять на вас кредит или похитить данные.

В специальной рубрике Объясняем.рф и Киберполиции России рассказываем, как вернуть контроль над аккаунтом и усилить его защиту.

Важно! Если мошенники успели сделать что-то от вашего имени, например подать заявление на выплату или оформить кредит, первым делом обратитесь в отдел полиции по месту жительства и сообщите о произошедшем в банки, где у вас есть счета.

▶Как восстановить доступ к Госуслугам

1. Попробуйте сбросить пароль:

на странице входа нажмите «Забыли пароль?» и следуйте инструкциям. Ссылка для сброса придёт на ваш e-mail или телефон, которые вы указали при регистрации.

2. Если мошенники успели сменить контактные данные, сброс не сработает. Тогда:

— восстановите доступ через приложение банка-партнёра;

— позвоните на горячую линию Госуслуг: 8 (800) 100-70-10;

— обратитесь в центр обслуживания.

▶После восстановления доступа:

— смените пароль на более надёжный — используйте комбинацию букв, цифр и символов;

— проверьте и обновите личнее данные (номер телефона, электронную почту или адрес), если они были изменены мошенниками;

— изучите историю операций, чтобы отследить подозрительные действия: запросы на выплаты или подачу заявлений;

— закажите кредитную историю, чтобы убедиться, что на вас не оформили заём.

▶Как защитить аккаунт на Госуслугах в будущем:

— Включите двухфакторную аутентификацию — при входе на ваш номер будет приходить СМС с кодом подтверждения.

— Укажите доверенный контакт в настройках безопасности. Это может быть кто-то из ваших близких или друзей. Ему отправят оповещение, если кто-то захочет сменить пароль.

Дополнительно поставьте самозапрет на кредиты — это можно сделать на Госуслугах или в МФЦ. Тогда мошенники не смогут взять заём на ваше имя, даже если получат ваши данные.