Как защитить себя от мошенников

сферум

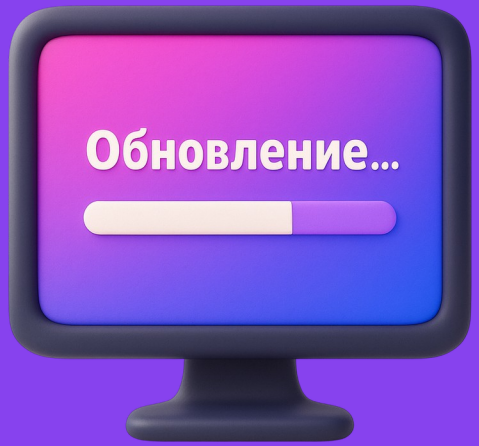
Правила информационной безопасности

1. Вовремя обновляйте программное обеспечение на телефоне и компьютере
2. Включайте антивирус
3. Используйте двухфакторную аутентификацию во всех сервисах
4. Создавайте сложные пароли
5. Выставляйте настройки приватности
6. Не переходите по подозрительным ссылкам и не открывайте сомнительные сообщения

1. Обновляйте программное обеспечение

Обновление программ, особенно системных, помогает закрывать уязвимости, которыми могут использовать злоумышленники.

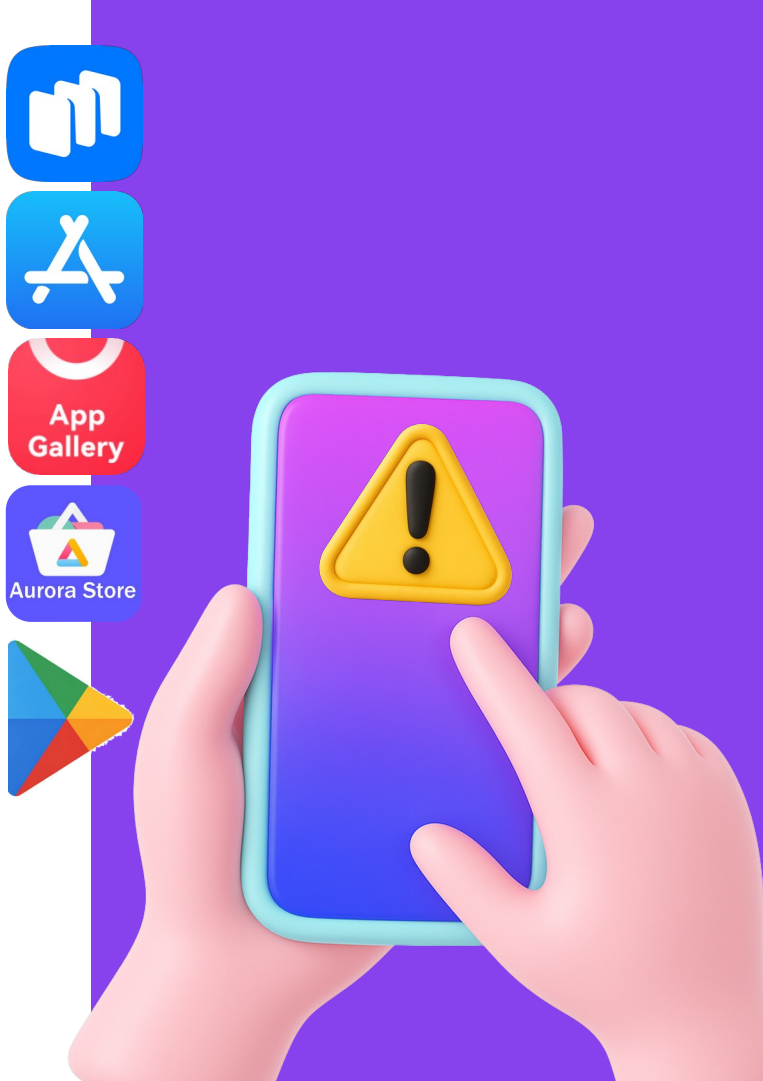
К обновлениям тоже нужно относиться внимательно — скачивайте их с официальных сайтов разработчиков. Если программа имеет собственную систему обновления — используйте её.



Обновляйте программное обеспечение из официальных источников

Мошенники используют поддельные мобильные приложения, чтобы воровать данные и деньги пользователей. Чаще всего их распространяют не через официальные магазины, а по ссылкам в интернете, в социальных сетях, через рассылки или даже в рабочих чатах.

www.max.ru



2. Включайте антивирус

Антивирусы помогают обнаружить вредоносные программы, которые снижают скорость работы вашего компьютера и крадут данные.

Виды вредоносных программ

- **Трояны.** Маскируются под существующие программы, например, под файл с браузером или игрой
- **Вирусы.** Встраиваются в другие программы и влияют на их работу
- **Шпионские программы.** Собирают и крадут информацию с компьютера
- **Руткиты.** Позволяют получить удалённый доступ к заражённому компьютеру

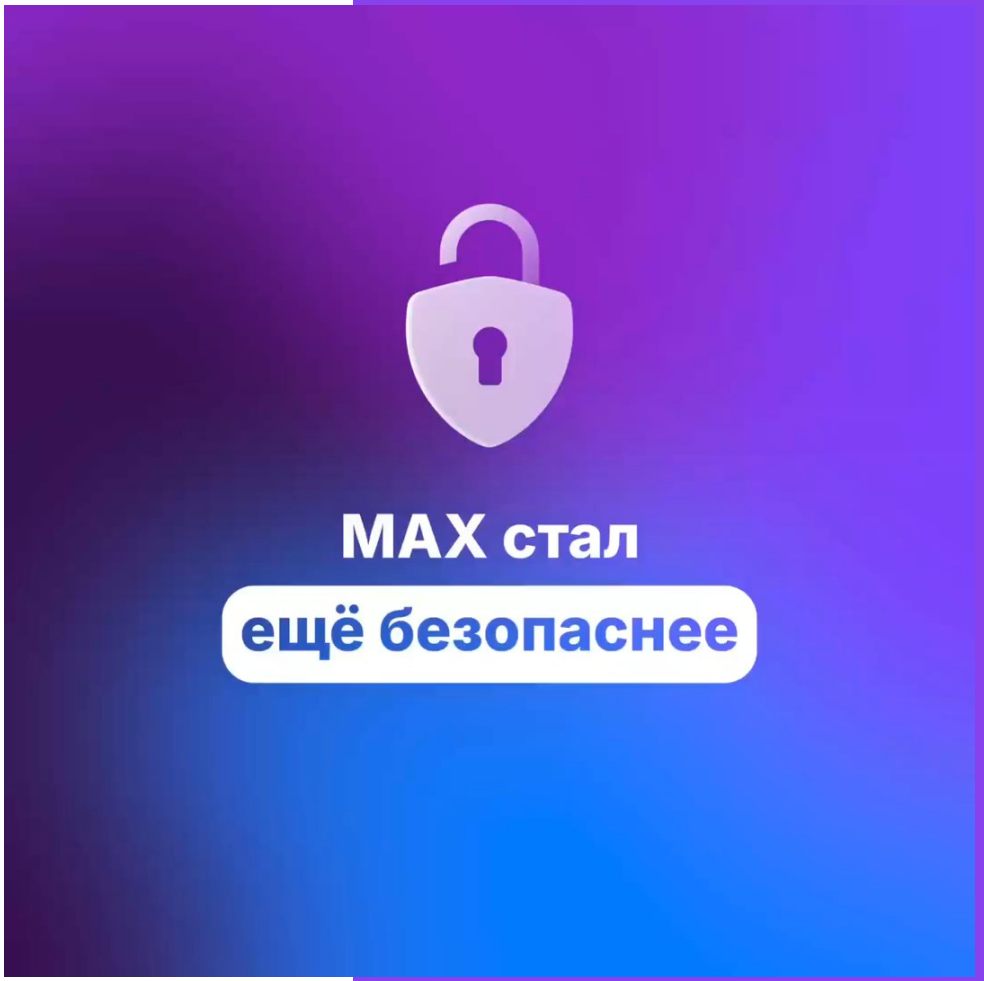
3. Используйте двухфакторную аутентификацию

Двухфакторная аутентификация защищает пользователя, так как кроме пароля, который может узнать мошенник, потребуется ввести ещё код из СМС или подтвердить личность иным способом.

Она доступна для множества сервисов: электронной почты, Госуслуг, банковских сервисов.

В Сферуме тоже есть двухфакторная аутентификация, подключить её можно в настройках приложения.

⚠️ **Сотрудники компаний НЕ просят сообщать коды из СМС, в отличие от мошенников**


MAX стал
ещё безопаснее

4. Создавайте сложные пароли

Каким должен быть пароль:

1. Сложным, но запоминающимся
2. Содержать больше 8 символов, а лучше 10–12 и больше: цифры, заглавные и строчные буквы, специальные символы (%, &, #)
3. Не повторяться в разных сервисах

Составить сложный пароль поможет специальный генератор, а сохранить его — менеджер паролей.

Как злоумышленники узнают пароли?

- **Перебор**. Программы комбинируют распространённые слова, используют их популярные сочетания, другие программы могут подобрать таким же образом цифровой пароль
- **Фишинг.** Мошенники могут попытаться выведать у вас важную информацию с помощью сайтов, писем или даже звонков
- **Утечки данных.** Утечки данных представляют для вас особенно большую угрозу, если вы используете один и тот же пароль в разных местах

Легко ли взломать ваш пароль

Количество символов	Только числа	Буквы в нижнем регистре	Буквы в нижнем и верхнем регистре	Числа, буквы в верхнем и нижнем регистре	Числа, буквы в верхнем и нижнем регистре, символы
4	Мгновенно	Мгновенно	Мгновенно	Мгновенно	Мгновенно
5	Мгновенно	Мгновенно	Мгновенно	Мгновенно	Мгновенно
6	Мгновенно	Мгновенно	Мгновенно	Мгновенно	Мгновенно
7	Мгновенно	Мгновенно	2 секунды	7 секунд	31 секунда
8	Мгновенно	Мгновенно	2 минуты	7 минут	39 минут
9	Мгновенно	10 секунд	1 час	7 часов	2 дня
10	Мгновенно	4 минуты	3 дня	3 недели	5 месяцев
11	Мгновенно	2 часа	5 месяцев	3 года	34 года
12	2 секунды	2 дня	24 года	200 лет	3 тыс. лет
13	19 секунд	2 месяца	1 тыс. лет	12 тыс. лет	202 тыс. лет
14	3 минуты	4 года	64 тыс. лет	750 тыс. лет	16 млн лет
15	32 минуты	100 лет	3 млн лет	46 млн лет	1 млрд лет
16	5 часов	3 тыс. лет	173 млн лет	3 млрд лет	92 млрд лет
17	2 дня	69 тыс. лет	9 млрд лет	179 млрд лет	7 трлн лет
18	3 недели	2 млн лет	467 млрд лет	11 трлн лет	438 трлн лет

3 шага для создания сложного пароля

1. Выберите парольную фразу из нескольких слов. Например: «Стол это вам не стул»
2. Замените буквы и пробелы на спецсимволы: «Ст0л_эт0_в@м_не_стУл»
3. Добавьте в получившийся пароль цифры: «Ст0л_эт0_в@м_не_стУл999»

Как хранить пароли

- Не записывайте пароли на листочках и в ежедневниках
- Не храните пароли в приложении «Заметки» на телефоне или в виде сообщения в чате «Избранное»
- Не сохраняйте пароли в браузере

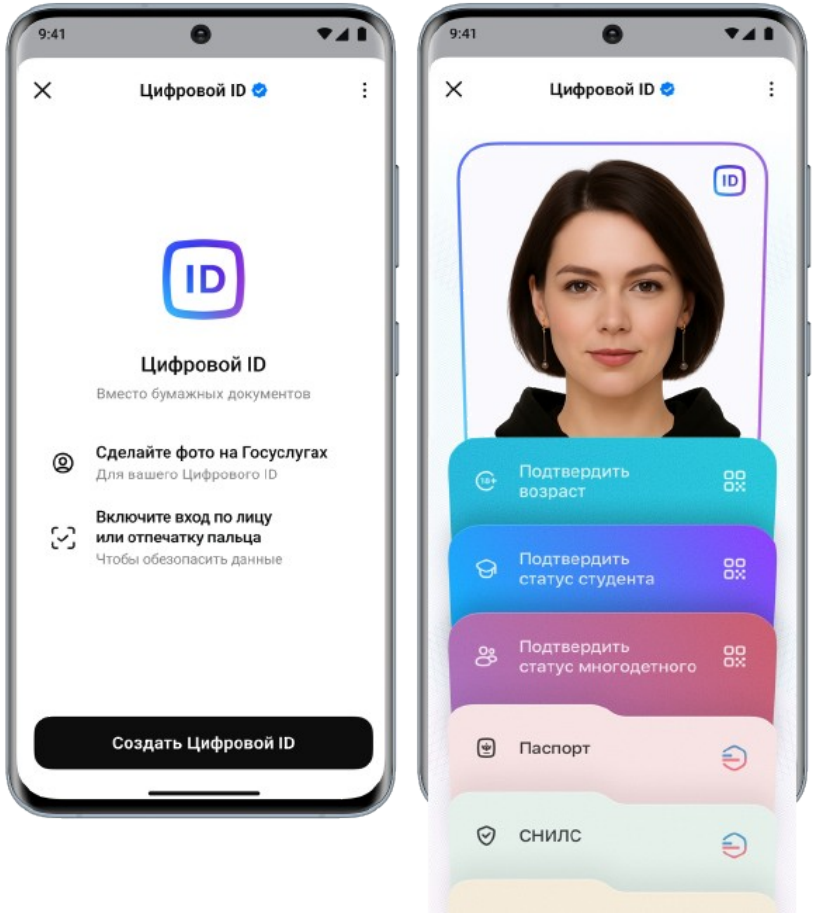
- Используйте менеджер паролей
- Используйте OnePass — системы быстрого входа без ввода пароля с помощью биометрии: по отпечатку пальца или по лицу

Чаще обновляйте пароли:

- банковских приложений
- социальных сетей
- мессенджеров
- электронной почты
- менеджера паролей

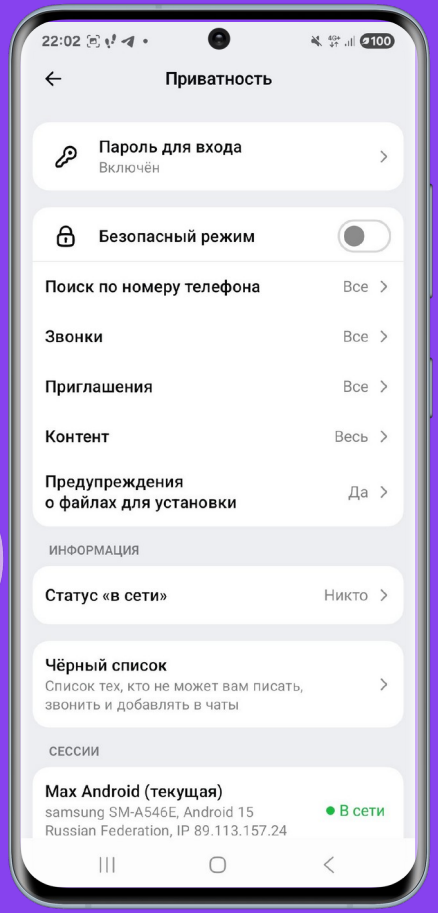
Как хранить свою информацию

- Цифровой ID в MAX – это аналог бумажных документов, с которыми можно подтвердить возраст, право на льготы и др.
- Цифровой ID невозможно передать или продать другому человеку — сервис действителен только на том устройстве, на котором он создавался;
- Доступ к QR-коду осуществляется только после биометрической проверки — через Face ID или по отпечатку пальца;
- При сканировании QR-кода персональная информация пользователя, в том числе дата его рождения, недоступна;
- Динамический QR-код обновляется каждые 30 секунд;
- Сделать скриншот Цифрового ID невозможно — вместо QR-кода на фото будет белый экран.



5. Выставляйте настройки приватности

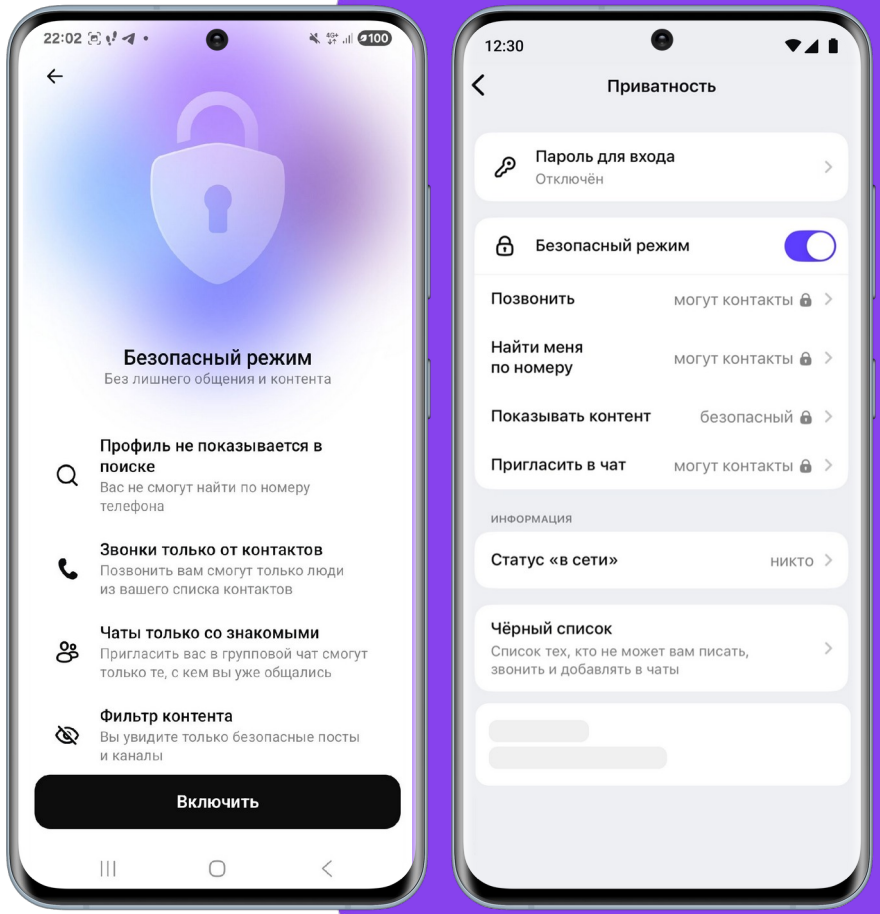
В настройках приватности или конфиденциальности в соцсетях и мессенджерах вы можете выбрать, какую информацию о вас будут видеть другие пользователи.



Безопасный режим

Режим включён по умолчанию у всех обучающихся

- → Звонить и приглашать в чаты могут только контакты из телефонной книги и учебной организации
- → Профиль нельзя найти по номеру телефона
- → Только безопасный контент в ленте, поиске и каналах



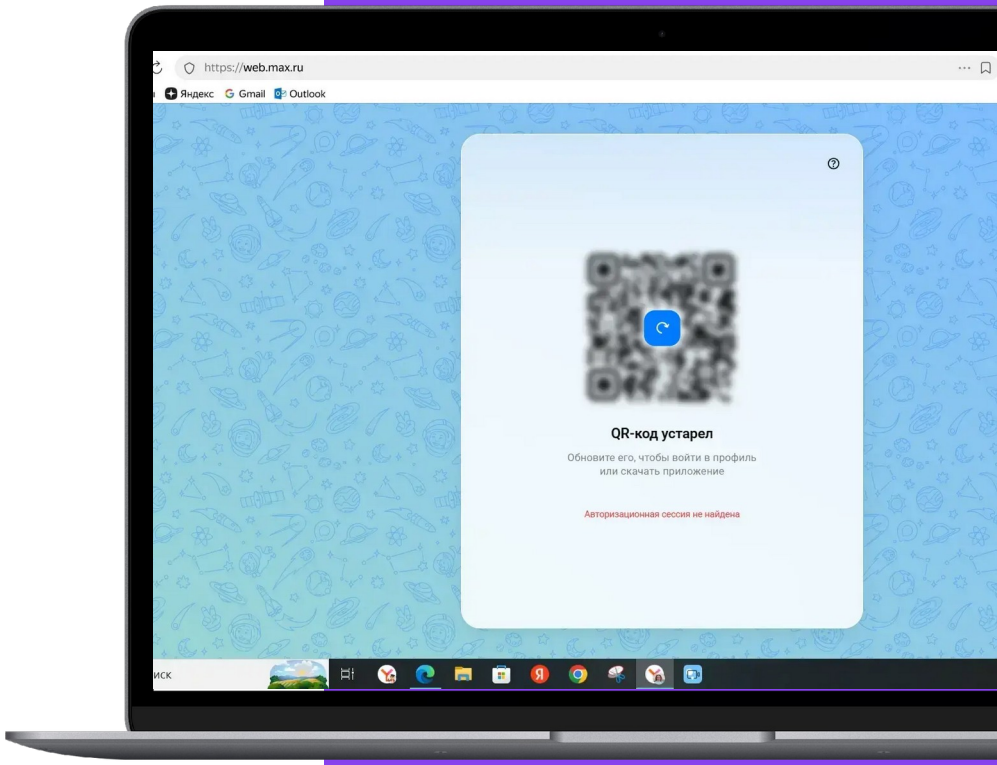
Семейная защита в MAX

Вход в web-версию MAX

Мы упростили вход для тех, кто предпочитает веб-версию Сферума в MAX.

Теперь достаточно открыть web.max.ru и отсканировать телефоном QR-код.

Для повышения безопасности проверка происходит внутри сервиса — это быстрее и надёжнее.



Правила безопасности в Сферуме

- Ссылки-приглашения для чатов и звонков отправляйте только в личных диалогах или через СМС — не размещайте их в социальных сетях или сообществах
- Используйте настройки привтности
- Удаляйте / обновляйте ссылки-приглашения после их использования
- **Используйте авточаты из РГИС или из Личного кабинета организации**
- Во время проведения звонков используйте зал ожидания для пользователей — вы сможете лично дать доступ к звонку каждому подключившемуся
- Включайте запись звонка и помните, вы можете отключать камеры и микрофоны у участников звонка

Обезопасить общение

Рекомендации по общению в чатах для педагогов

- *Подскажут, как выстроить безопасное общение в учебных чатах, и дадут пошаговые инструкции*

Советы родителям, как обезопасить чаты

- *Дадут пошаговые инструкции, как защитить переписки ребёнка, и расскажут о методах интернет-безопасности*

Памятка по интернет-безопасности для детей

- *Поможет создать защищённое пространство для детей, предупредит об основных опасностях и подскажет, как действовать педагогам, родителям и ученикам*

Общая памятка по безопасности в сети

- *Даст рекомендации, как защитить свою персональную информацию в интернете*

www.prof.sferum.ru

Памятки по безопасности

Как подготовиться к обновлению гаджета

1. Скопируйте важную информацию со старого устройства
2. Убедитесь, что вы вышли из всех учетных записей, которые есть на гаджете
3. Проверьте не остались ли в гаджете SIM-карты или карты памяти
4. После того, как вы скопировали со старого устройства все необходимые данные, сделайте сброс к заводским настройкам или вручную удалите всю информацию на гаджете

Если вы потеряли телефон

1. Заблокируйте SIM-карту через оператора связи
2. Получите в салоне мобильной связи новую SIM-карту со старым номером
3. Переустановите все пароли

С чем могут столкнуться дети в сети

1. **Звонки от неизвестных**
   Напомните ребёнку, что звонки с незнакомых номеров нужно сбрасывать, а звонящих отправлять в чёрный список
2. **Угрозы и запугивание**
   Расскажите, как вести себя в подобных ситуациях: сделать скриншот сообщения, отправить жалобу и заблокировать пользователя
3. **Предложение помощи в играх или заработка внутриигровых валют**
   Обсудите, что это — часть мошеннических схем, чтобы получить доступ к личным данным ребёнка и его родителей
4. **Просьбы поделиться фотографиями, личными данными (своими, друзей, родителей и учителей)**
   Научите, что такие просьбы нужно пресекать, даже если их отправляют с аккаунтов знакомых

Памятка по безопасности детей

Фишинг и социальная инженерия

Мошенник:

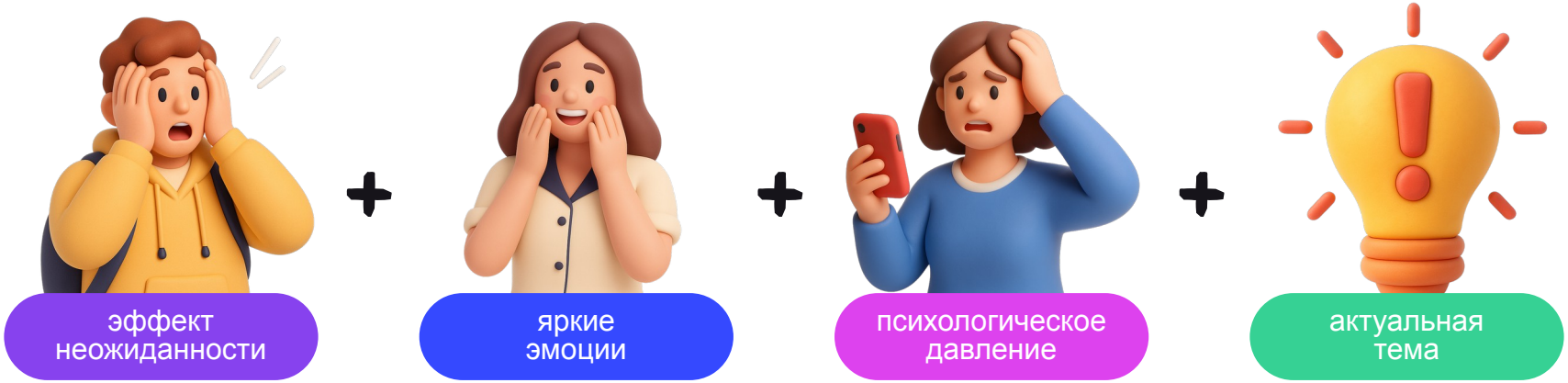
- Хорошо разбирается в видах психологического воздействия
- Умеет манипулировать
- Подготовлен

Мошенник хочет получить:

- Логин и пароль
- Данные для двухфакторной аутентификации
- Код из СМС
- Данные банковской карты
- Пин-код
- Ваши деньги и имущество

Российские интернет-пользователи каждый день пытаются перейти на фишинговые ресурсы примерно 1,5 млн раз, в 90% случаев это переходы с мобильного телефона, в том числе из мессенджеров, писем и приложений

Фишинг и социальная инженерия

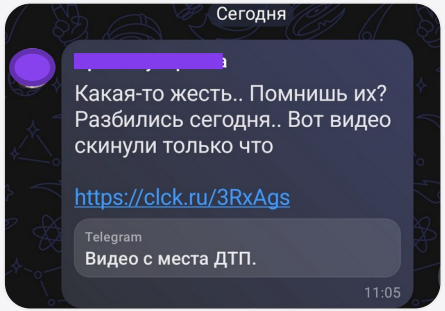


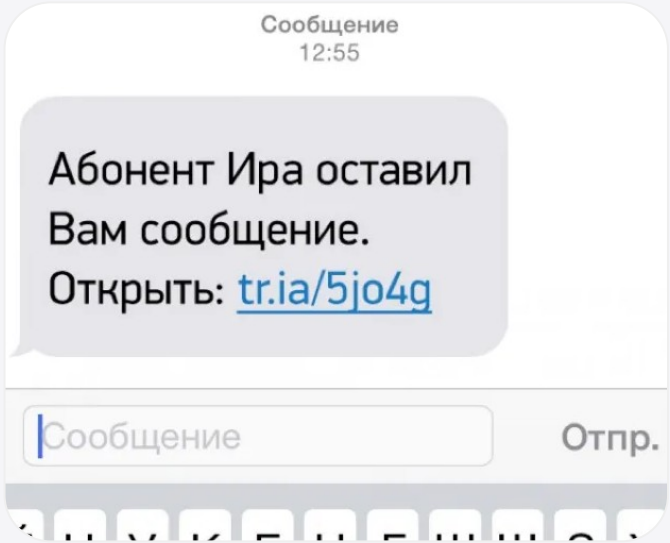
Мошенники используют человеческие слабости

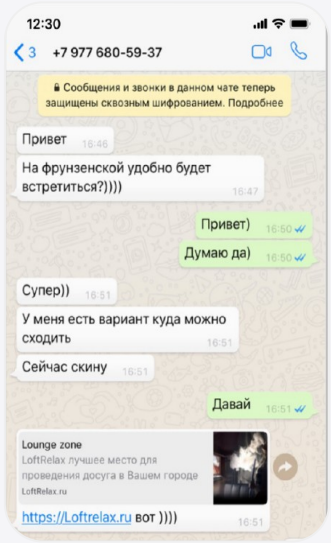
В итоге человек готов сделать всё, о чём его попросят

Фишинг и социальная инженерия

Любопытство





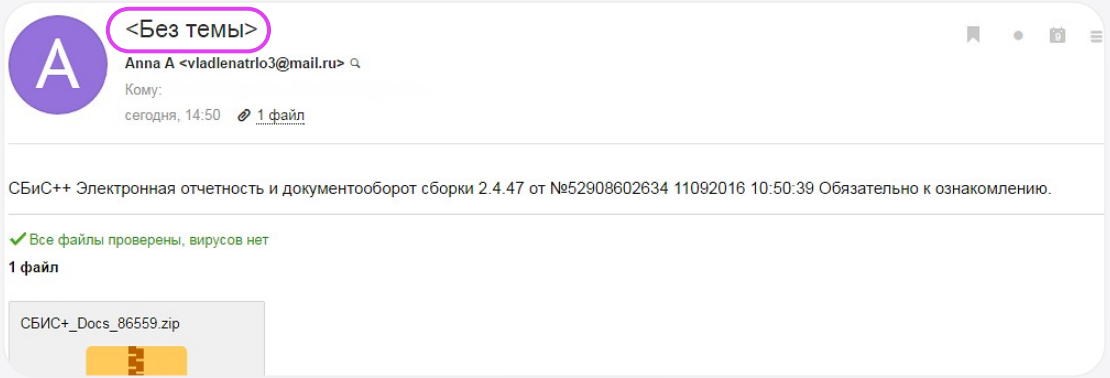


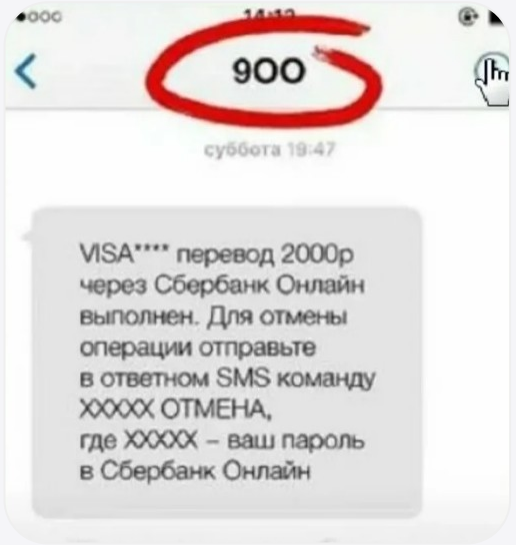
Фишинг и социальная инженерия

Невнимательность

https://max.ru

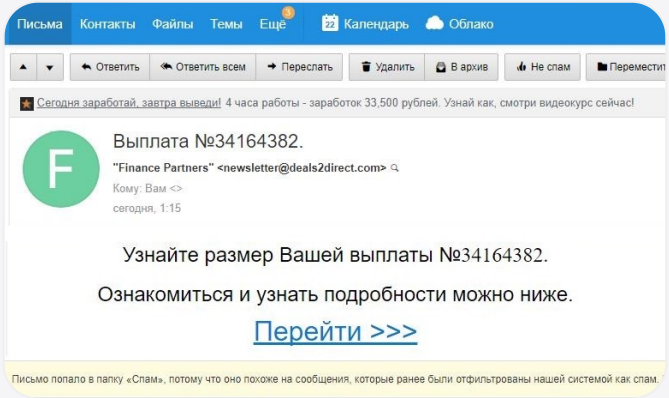
https://rnax.ru

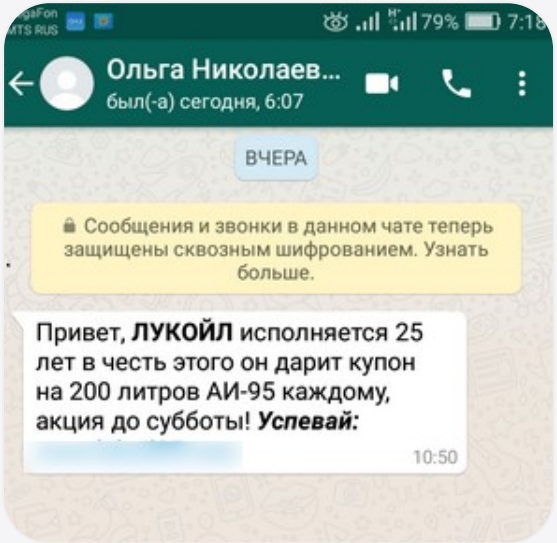




Фишинг и социальная инженерия

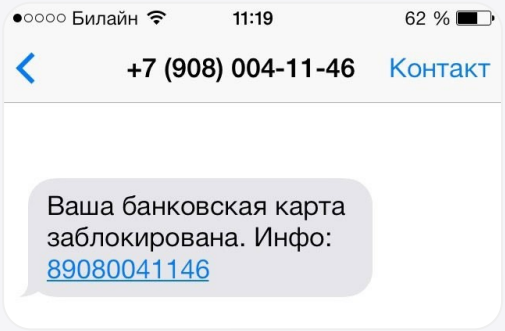
Надежда, желание получить деньги

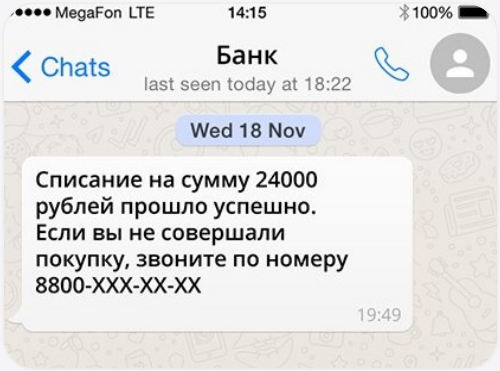


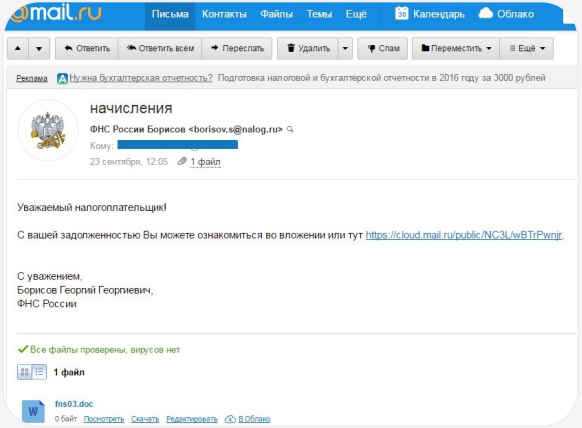


Фишинг и социальная инженерия

Страх, паника, чувство стыда



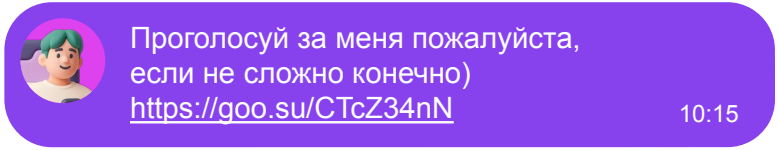




Фишинг и социальная инженерия

Как это работает

Злоумышленник пишет вам, используя учётную запись вашего друга или знакомого:

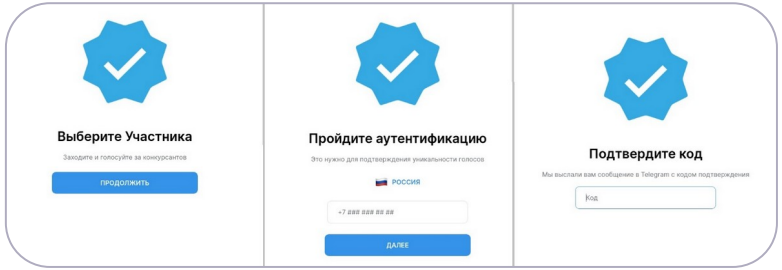


Ссылка, отправляемая злоумышленниками, сделана при помощи сервиса для сокращения ссылок.

Этот инструмент часто применяется, когда отправитель не хочет, чтобы реальный адрес сайта бросался в глаза.

Сайт злоумышленников

Указав номер телефона, вы получите код подтверждения, с помощью которого у вас украдут данные учётной записи.



Схемы работы мошенников

- Сотрудниками почтовых сервисов и служб доставки и **сообщают о якобы поступившем письме (документах)**. Легенды меняются — «сортировочный центр», «служба доставки», «налоговая инспекция», «оператор связи», «МФЦ» и др.
- **Мошенничество с инвестициями.** Схема начинается с рекламы «выгодных вложений», которую распространяют в соцсетях и мессенджерах. Чтобы вызвать доверие, аферисты используют фото и видео популярных блогеров, якобы «рекомендующих» новый способ заработка.
- **Мошенничество на онлайн-площадках**: фейковая бронь товара, поддельная доставка и т.д.
- **Оцифровка архивов**: поддельные чаты в мессенджерах, в которых идет коммуникация якобы с начальником и коллегами (текущими / бывшими)
- **Объявления с QR-кодом** для вступления в соседский чат
- **Сообщения о проверках на текущей/бывшей работе**

Схемы работы мошенников

- **Рассылка фейковых писем якобы от «Госуслуг»** с уведомлением о входе в аккаунт с другого устройства. В письме название портала написано с ошибкой ("Gos uslugi") и указан поддельный номер поддержки, по которому предлагают "срочно связаться".
- **Замена домофона. Замена/проверка счетчиков**
- **Установка на телефон приложения** для управления новым домофоном
- **Запись в поликлинику** для прохождения диспансеризации, **запись в социальный фонд** для оформления положенных выплат
- **Обновление договора с оператором связи**
- «**Заработок на лайках**». Предлагается «лёгкий и быстрый заработок» — ставить лайки на товары в интернет-магазинах и получать за это деньги.

Правила защиты от фишинга

На что обратить внимание

1. Сообщение неожиданное?
2. От кого пришло сообщение? Знаком ли вам отправитель?
3. Вызывает ли сообщение яркие эмоции — страх, волнение, панику?
4. Есть ли в сообщении акцент на срочность?
5. Содержит ли сообщение потенциально опасные вложения?

Правила защиты от фишинга

1. Не доверяйте никому и ничему. Если есть подозрение, что пришедшее уведомление, письмо или сайт являются подлинным, лучше перепроверьте его
2. Проверяйте адреса и ссылки в сообщении, они могут быть подделаны
3. Не нажимайте на все ссылки и баннеры, которые видите. А если что-то открыли — не вводите персональные данные

Часто хакеры искусственно увеличивают размер прикрепленного к фишинговому сообщению файла, например до 600 или 700 МБ. Из-за ограничений антивирусов на размер проверяемого файла такое вложение может проскочить через защиту.

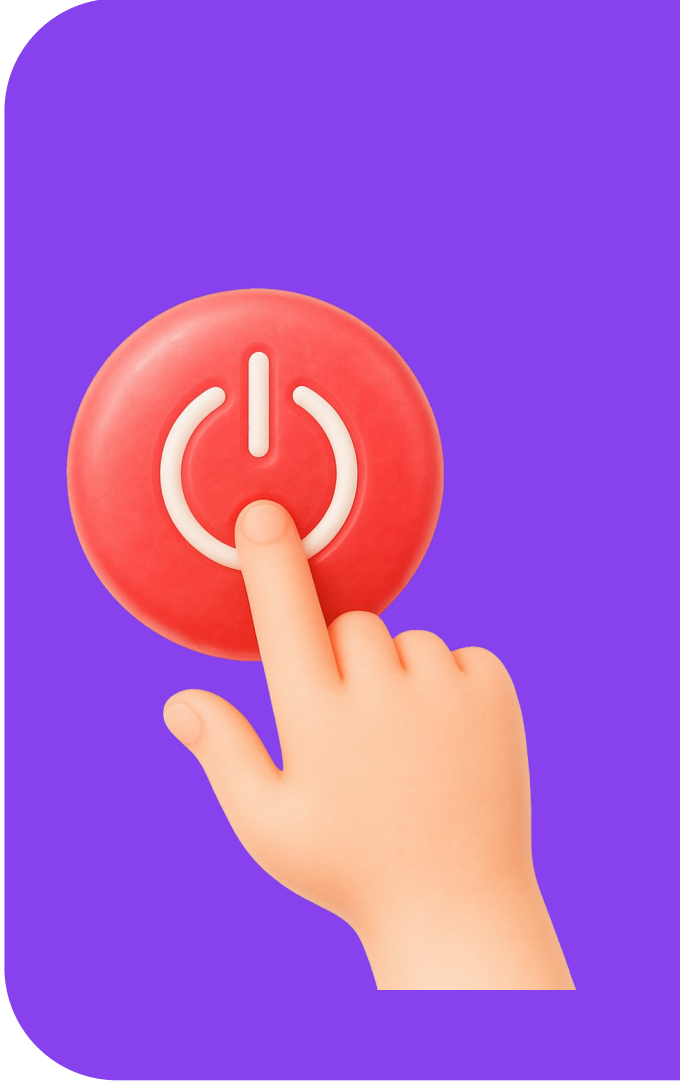
Обращайте на это внимание, вложенный документ вряд ли будет занимать больше 20 Мб, даже если это презентация.

Также обращайте внимание на формат, полученного файла.

Правила защиты от фишинга

Если вы перешли по ссылке от мошенника

1. Не торопитесь с дальнейшими действиями, подумайте
2. Внимательно отнеситесь к полученному контенту и включите критическое мышление
3. Обратитесь за уточнением к друзьям, службе безопасности или другой организации от имени которой вы получили сообщение — точно ли это предложение поступило от них
4. Завершите сеансы на всех устройствах в приложениях, которыми пользуетесь
5. Оставьте жалобу на поступивший контент, заблокируйте пользователя и добавьте адрес отправителя в черный список



VPN

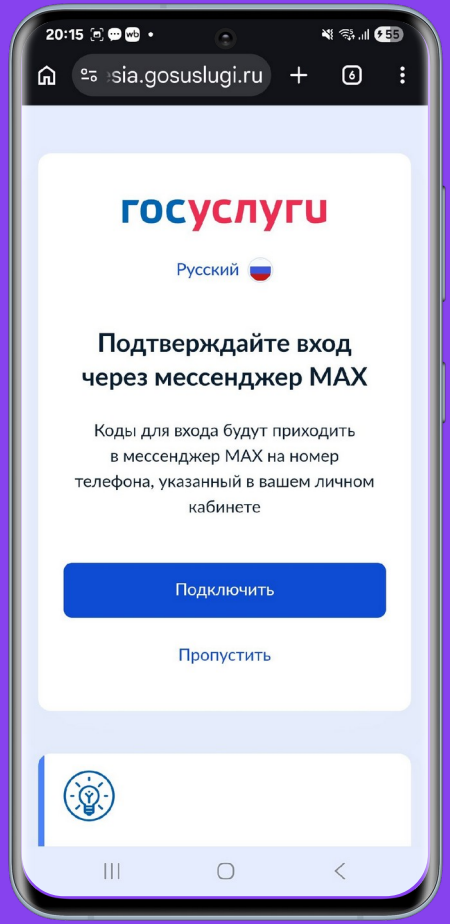
1. Использование VPN при работе с банковскими приложениями, может привести к блокировке личного кабинета
2. В некоторых случаях VPN-приложения могут анализировать действия пользователя для продвижения рекламного контента. В худших сценариях под видом VPN-сервисов может быть внедрено вредоносное ПО
3. VPN-сервисы также лучше не использовать при входе в личные аккаунты в социальных сетях, чтобы обезопасить свои персональные данные
4. Проверяйте VPN-приложения перед установкой антивирусом

Теперь вы в безопасности

1. Не используем VPN при работе с банковскими приложениями — это может привести к блокировке личного кабинета
2. Обновляем вовремя программное обеспечение
3. Используем антивирусы
4. Устанавливаем двухфакторную аутентификацию
5. Создаём сложные пароли
6. Не храним пароли у всех на виду и в легкодоступных местах
7. Пользуемся настройками конфиденциальности и приватности
8. Выходим из своего профиля на устройствах, которыми могут воспользоваться другие люди
9. Не передаём доступ к своему телефону чужим людям
10. В случае потери телефона — блокируем SIM-карту через оператора
11. С осторожностью используем открытые Wi-Fi-сети и Bluetooth ссоединенеия

Госуслуги и информационная безопасность

«Из-за растущего числа случаев мошенничества, когда пользователи Госуслуг непреднамеренно передают СМС-коды для входа на портал, было принято решение постепенно отказаться от подтверждения входа на портал через СМС — пока это решение касается только входа на «Госуслуги» через мобильные устройства.»



Госуслуги и информационная безопасность

С помощью Госуслуг вы можете ещё лучше себя обезопасить себя:

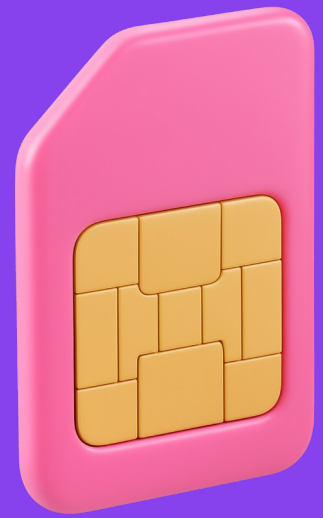
- установить запрет на действия с вашим имуществом без личного присутствия
- узнать, какие сим-карты на вас зарегистрированы, и расторгнуть договор на их обслуживание в случае необходимости
- найти информацию, в каких бюро хранится ваша кредитная история
- установить запрет на заключение с вами кредитных договоров

Информация о сим-картах

В разделе «Сим-карты» на Госуслугах отображаются личные и корпоративные номера телефонов. Раздел доступен для граждан с 14 лет с подтверждённой учётной записью.

По каждому номеру в разделе есть информация. Вы можете присвоить номеру уникальное название. Если вы обнаружите номер, на который не оформляли договор, то сможете заблокировать его или расторгнуть договор.

Также Вы можете устновтьи **Запрет на оформление договоров на оказание услуг мобильной связи**. Снять его можно будет в МФЦ



Запрет регистрационных действий без присутствия собственника

На Госуслугах вы или ваш законный представитель можете подать заявление о запрете государственной регистрации **перехода, прекращения, ограничения права и обременения объекта недвижимости** без личного участия.

Вам потребуются:

- паспортные данные
- ИНН
- кадастровый номер объекта недвижимости

Заявление необходимо подписать усиленной квалифицированной цифровой подписью через приложение «Госключ» в течение 24 часов с момента отправки.

Запись о запрете регистрации будет внесена в ЕГРН в течение 5 рабочих дней со дня приёма заявления. Уведомление об этом придет в личный кабинет.

Поиск бюро с вашей кредитной историей

Услуга поможет узнать список бюро кредитных историй (БКИ), в которых хранится ваша кредитная история.

В личных кабинетах найденных БКИ вы сможете запросить кредитную историю и узнать свой индивидуальный кредитный рейтинг.

Запрет на заключение кредитных договоров

После установления такого запрета никто не сможет взять кредит на ваше имя.

Если финансовая организация заключит договор с человеком, у которого установлен запрет, он не будет нести за него ответственность и все обязанности по выплате кредита перейдут к финансовой организации.

Аккаунт в мессенджерах – ваша цифровая собственность!

С 1 сентября 2025 года за передачу посторонним своих учётных записей (включая игровые, в соцсетях и мессенджерах) и сим-карт за деньги грозит штраф и уголовная ответственность. Если через ваш аккаунт произведут мошеннические операции, отвечать придётся именно вам. Аккаунт — это не товар, а ваша цифровая личность. Никогда не отдавайте его в чужие руки.

За передачу аккаунтов может грозить административный **штраф до 700 тыс. руб. и уголовная ответственность (лишение свободы до двух лет)** в некоторых случаях, таких как участие в мошеннических схемах.

Федеральный закон от 31.07.2025 № 281-ФЗ

Что делать если меня заблокировали в MAX?

Необходимо оформить обращение в службу технической поддержки (СТП) MAX через сайт max.ru

В обращении необходимо:

- → Представиться: назвать ФИО, организацию и вашу роль (должность) в организации (для обучающихся – указать класс / курс)
- → Указать номер телефона. Желательно в формате 7**********
- → Сообщить о действиях, которые привели к блокировке
- → Приложить изображение (видео), на котором видно, что устройство проверено на вирусы и их нет

Техподдержка MAX
https://help.max.ru

Центр безопасности MAX

Оперативно реагирует на жалобы пользователей

За январь 2026 года

- предотвращена передача 25 тысяч вредоносных APK-файлов, заблокировано 230 тысяч подозрительных аккаунтов и удалено 2,2 миллиона вредоносных файлов
- 17 человек удалось вовремя вывести из-под влияния злоумышленников и тем самым сохранить гражданам более 22 миллионов рублей
- Совместно с МВД России были раскрыты три преступления и задержаны четверо подозреваемых в мошенничестве.

Центр безопасности MAX

Спасибо
за внимание!

сферум