Министерство цифрового развития и связи
Оренбургской области

digital.orb.ru

ПРАВИЛА ПРОТИВОДЕЙСТВИЯ ПОПЫТКАМ ВЗЛОМА В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ, А ТАКЖЕ ФИШИНГОВЫМ АТАКАМ

Оренбургская область
2026 г.

Что такое фишинг?

Фишинг (на англ. phishing-рыбная ловля, выуживание) – один из популярных видов мошенничества в интернете , целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям, данным кредитных карт, номерам телефонов. Паспортным данным и т.д Жертвами фишинга чаще всего становятся:

44%

госучреждения

19%

оборонные предприятия

14%

организации в сфере науки и образования

Цели:

- **Украсть персональные данные**. Логины, пароли, номера банковских карт, паспорта, ИНН используют для кражи личности, оформления кредитов на имя жертвы, получения доступа к личным аккаунтам и продажи полученных данных третьим лицам.

- **Получить доступ к банковским счетам**. Чтобы совершать несанкционированные переводы, покупки и другие финансовые операции.

- **Распространить вредоносное ПО**. Вирусы, трояны, шпионское ПО через вложения в сообщениях или ссылки, чтобы вывести из строя инфраструктуру учреждения

- **Получить корпоративную информацию**. Специальные фишинговые атаки на компании и организации нацелены на кражу деловой информации, данных клиентов, финансовых отчётов и других конфиденциальных данных.

- **Украсть деньги**. Финансовое мошенничество позволяет злоумышленникам напрямую обогащаться за счёт жертв и отмывать деньги через перевод на подставные счета.

- **Получить выкуп**. Программы-вымогатели шифруют учётные данные жертвы и требуют выкуп за их восстановление.

Виды фишинга

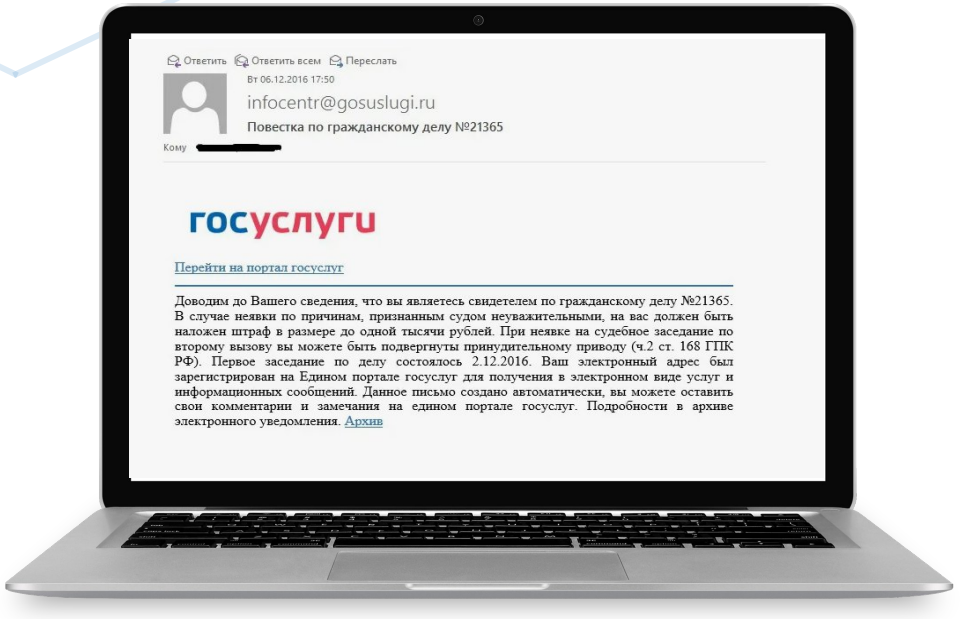
- **почтовый**
- **Spear Phishing (спеарфишинг или целевой фишинг)**
- **Whaling (уэйлинг)**
- **Smishing (смишинг)**
- **Vishing (вишинг)**
- **Evil Twin Phishing (фишинг-атака «злой двойник»)**
- **Фишинг в социальных сетях**
- **Вредоносное ПО**

1.Почтовый фишинг

Почтовый фишинг – один из самых распространенных типов фишинга.

Часто хакеры массово отправляют письма на максимально возможное количество адресов.

Такие письма зачастую содержат характер срочности, например, сообщая получателю, что его личный счет был взломан, а потому он должен немедленно ответить. Их цель заключается в том, чтобы своей срочностью вызвать необдуманное, но определенное действие от жертвы, например, нажать на вредоносную ссылку, которая ведет на поддельную страницу авторизации.



Киберучения проводимые министерством цифрового развития и связи Оренбургской области в 2025 году

29 января 2025 года

Тема письма: «Ознакомление с расчетными листами 1С Кабинет сотрудника»

Письмо содержало замаскированную ссылку после перехода по ней открывалась форма замаскированная под 1с (ГИС ФХД), содержащая кнопку для скачивания условно вредоносного файла. После нажатия на кнопку производилось скачивание условно вредоносного файла, запуск которого приводил к имитации заражения автоматизированного рабочего места, что в условиях реальной атаки могло бы повлечь заражение остальных устройств в сети Правительства Оренбургской области.

Начало рассылки 07:00

1840
Всего писем

147
(~11% от общего)
Открыли письма

118
(~80% от открытых писем)
Перешли по ссылке

23 раза
(~16% от открывших письмо)
Открыли вредоносный файл

30 мая 2025 года

Тема письма: (без темы)

Письмо содержало замаскированную ссылку после перехода по ней скачивался условно вредоносного файл. После нажатия на кнопку производилось скачивание условно вредоносного файла, запуск которого приводил к имитации заражения автоматизированного рабочего места, что в условиях реальной атаки могло бы повлечь заражение остальных устройств в сети Правительства Оренбургской области.

Начало рассылки 07:00

1840
Всего писем

57
(~47% от общего)
Открыли письма

121
(~6,6% от открытых писем)
Перешли по ссылке

29 раз
(~50% от открывших письмо)
Обратились к вредоносному серверу

30 июля 2025 года

Тема письма: «Обновление системы АСЭД»

Письмо содержало замаскированную ссылку после перехода по ней открывалась форма замаскированная под Портал поддержки электронного правительства Оренбургской области, содержащая кнопку для скачивания условно вредоносного файла. После нажатия на кнопку производилось скачивание условно вредоносного файла, запуск которого приводил к имитации заражения автоматизированного рабочего места, что в условиях реальной атаки могло бы повлечь заражение остальных устройств в сети Правительства Оренбургской области.

Начало рассылки 07:00

150
Всего писем

89
(~5,7% от общего)
Открыли письма

11
(~12% от открытых писем)
Перешли по ссылке

3 раза
(~27% от открывших письмо)
Запустили вредоносный файл

17 ноября 2025 года

Тема письма: О вступлении в силу приказов Минздрава РФ №215н, №216н "О выборе медицинской организации"

Письмо содержало замаскированную ссылку после перехода по которой, открывалась форма для заполнения данных, после отправки которой осуществлялось скачивание условно вредоносного файла, запуск которого приводил к имитации заражения автоматизированного рабочего места, что в условиях реальной атаки могло бы повлечь заражение остальных устройств в сети Правительства Оренбургской области.

Начало рассылки 20:00

1934
Всего писем

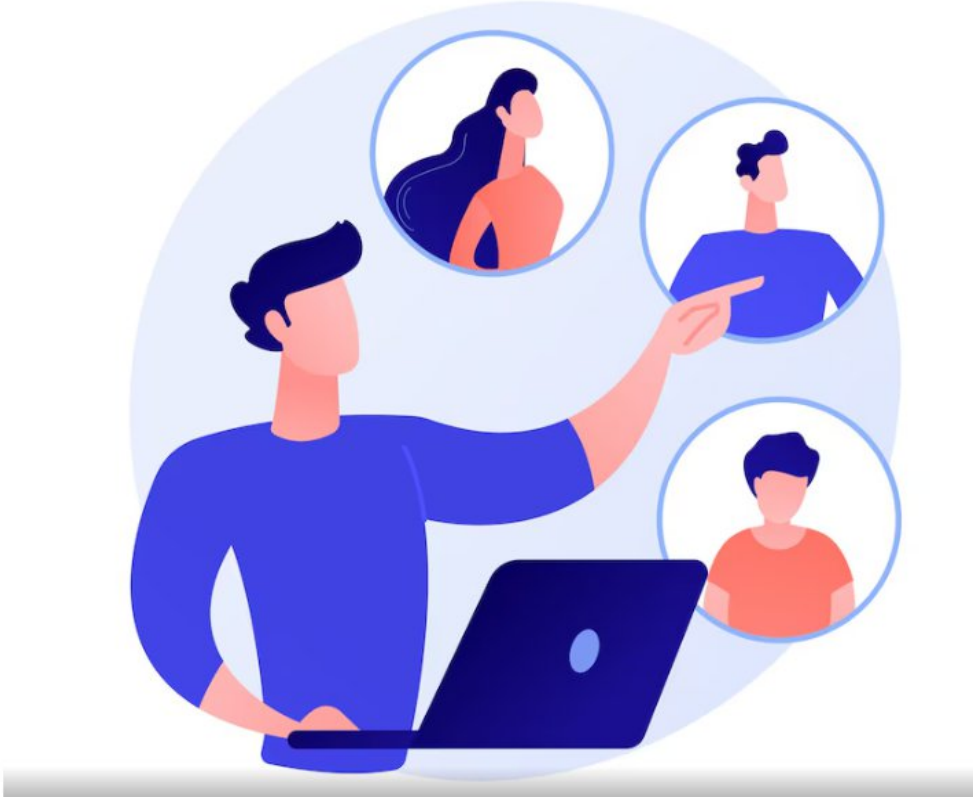
61
(~3,1% от общего)
Открыли письма

41
(~67,2% от открытых писем)
Перешли по ссылке

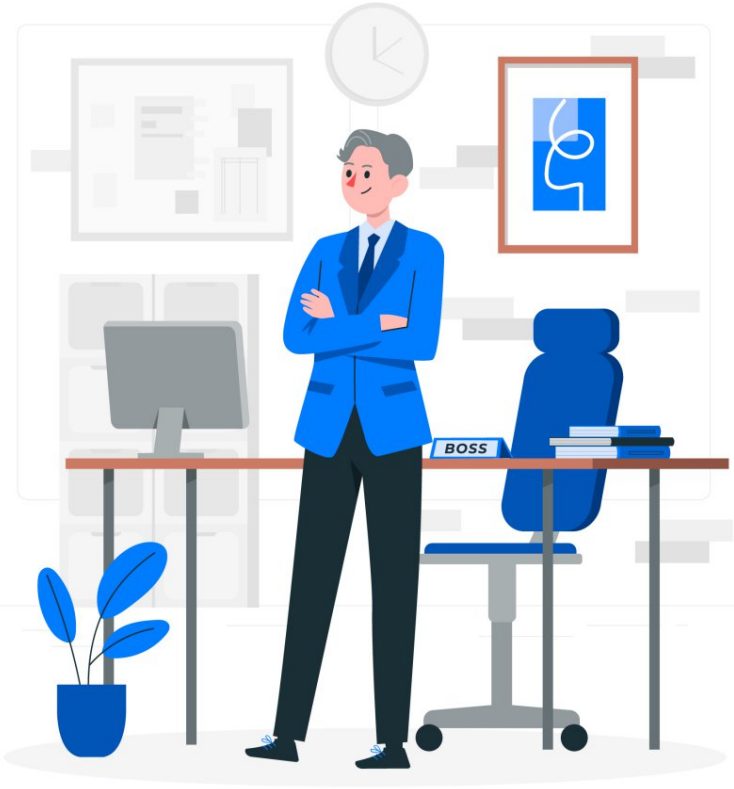
19 раз
(~46,3% от открывших письмо)
Обратились к вредоносному серверу

2. Spear Phishing (спеарфишинг или целевой фишинг)

Спеарфишинг включает в себя отправку вредоносных электронных писем конкретным лицам внутри организации. Вместо того, чтобы рассылать массовые электронные письма тысячам получателей, этот метод нацелен на определенных сотрудников в специально выбранных компаниях. Такие типы писем часто более персонализированы, они заставляют жертву поверить в то, что у них есть отношения с отправителем.



2. Whaling (уэйлинг)

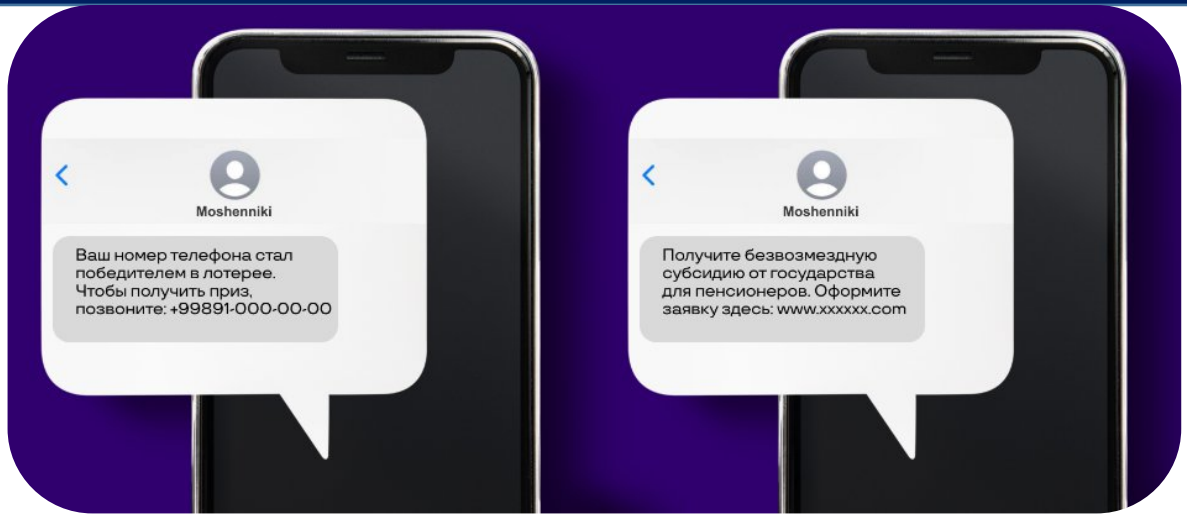


Whaling (уэйлинг) очень похож на spear phishing (спеарфишинг), но вместо того, чтобы преследовать любого сотрудника в компании, мошенники специально нацеливаются на руководителей.

К таким сотрудникам относятся генеральный директор, финансовый директор или любой руководитель высокого уровня, имеющий доступ к более конфиденциальным данным, чем сотрудники более низкого уровня. Часто эти электронные письма используют ситуацию, способную оказать на таких руководителей серьезное давление, чтобы «зацепить» своих потенциальных жертв, например, передавая информацию о поданном против компании судебном иске. Такое письмо побуждает получателя перейти по вредоносной ссылке или к зараженному вложению для получения дополнительной подробной информации.

3. Смишинг

SMS-фишинг, или smishing (смишинг), для проведения фишинговой атаки использует текстовые сообщения, а не электронную почту. Принцип действия такой же, как и при осуществлении фишинговых атак по электронной почте: злоумышленник отправляет текстовое сообщение от, казалось бы, легитимного отправителя (например, заслуживающая доверия компания), которое содержит вредоносную ссылку. Ссылка может быть замаскирована под код купона (скидка 20% на ваш следующий заказ!) или предложение выиграть что-то вроде билетов на концерт.



Как Миша стал жертвой мошенничества, получив СМС о покупке, которую он не совершал

Миша получил уведомление о том, что с его карты были списаны деньги за покупку, которую он не совершал. В конце СМС указан номер телефона банка, на который нужно позвонить, чтобы отменить платеж, либо перейти для этого по ссылке.

(Получено СМС следующего содержания)

13:00

Оплата в размере 2300 рублей с карты ****. Чтобы отменить данную покупку, пожалуйста, перезвоните по указанному номеру телефона или перейдите по ссылке.

13:05

...

(Миша позвонил по номеру из сообщения)

13:07

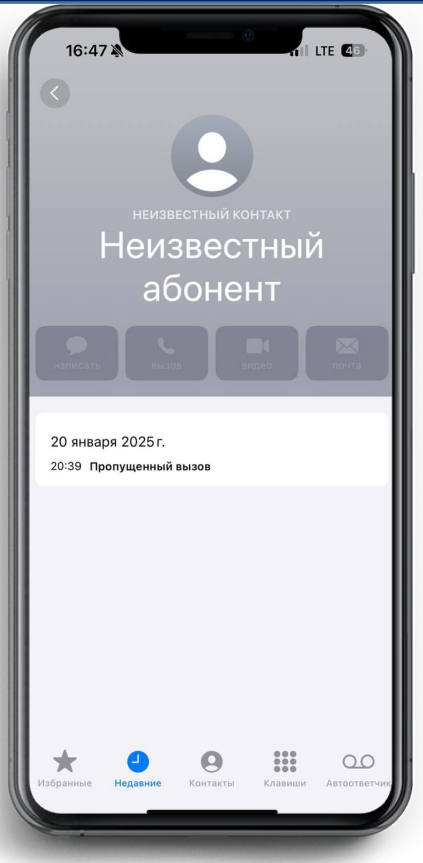
Михаил, добрый день! Не волнуйтесь. Чтобы банк отменил покупку и вернул вам средства, следуйте моим инструкциям: сообщите мне номер вашей карты, срок действия, имя владельца и CVC/CVV-код. Только так мы сможем однозначно подтвердить вашу личность и отменить последнее списание.

4. Вишинг (голосовой фишинг)

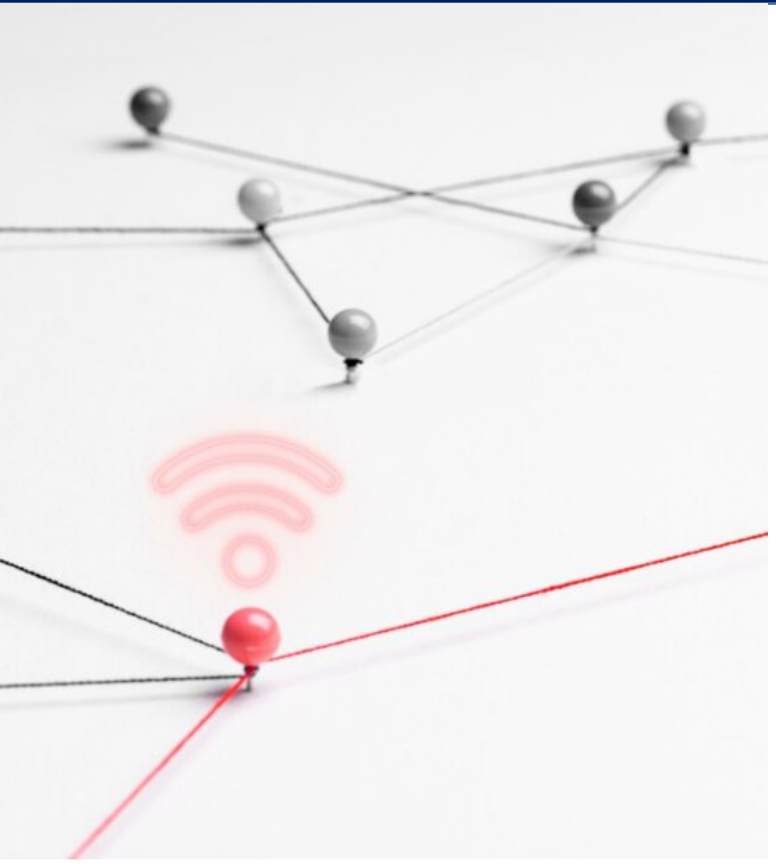
Голосовые атаки производятся с помощью телефонного звонка. Атака передает автоматическое голосовое сообщение якобы от банка или гос. учреждения. Злоумышленники заявляют, что вы задолжали крупную сумму или имеете неоплаченный штраф. Обговариваются сроки обязательного платежа и санкции в случае его отсрочки.

Например, под видом известных телекоммуникационных компаний мошенники стараются получить доступ к аккаунту пользователя Госуслуг. Они звонят жертве и утверждают, что действующий договор заканчивается и его необходимо продлить, иначе номер заблокируется. Чтобы никуда не идти, мошенники предлагают сделать все по телефону, продиктовав код из СМС.

Важно! Договоры, заключаемые абонентом с сотовыми операторами, не предусматривают ограниченного срока использования номером.



“Злой двойник”

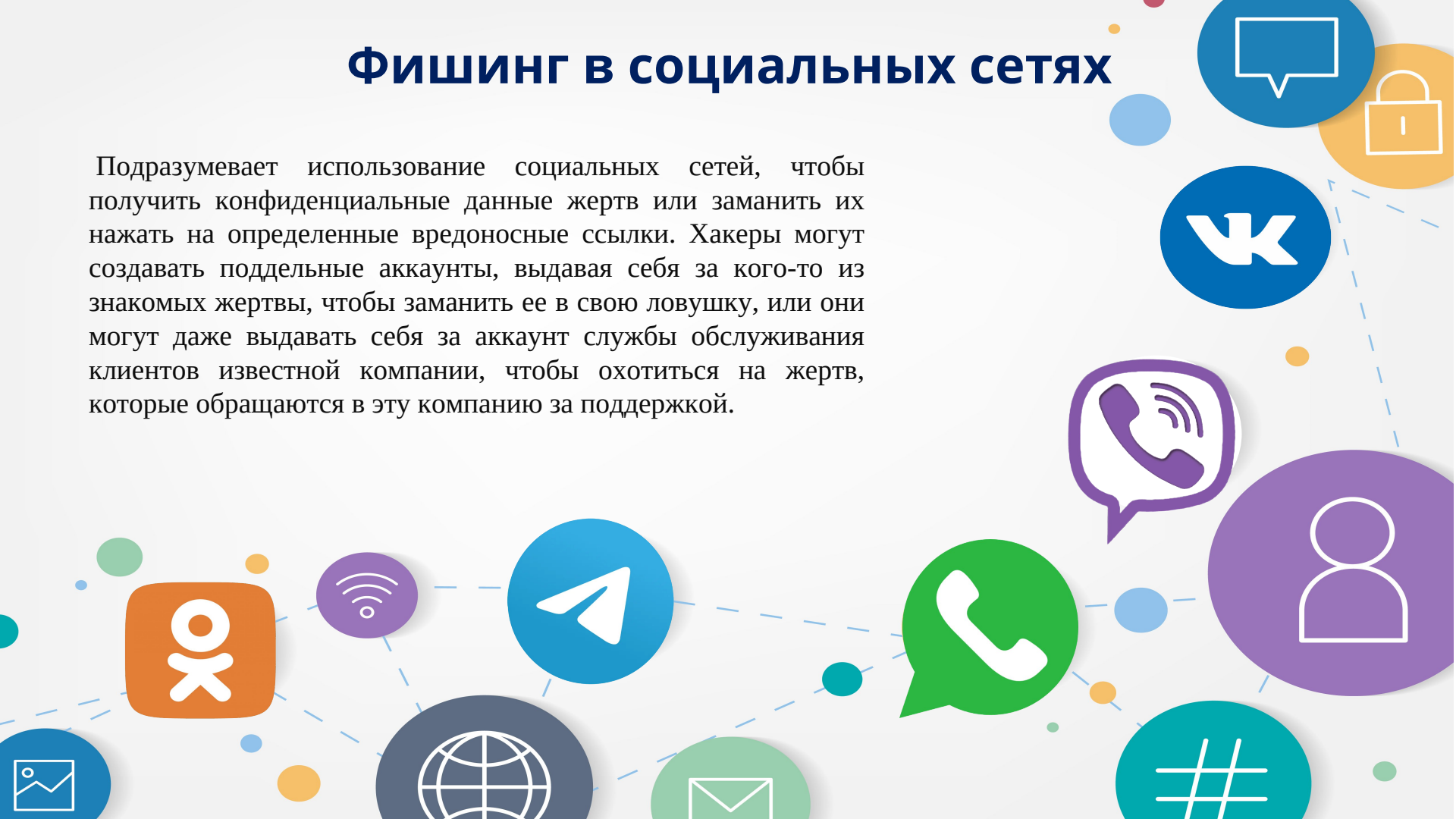


Эта кибератака заключается в создании ненастоящей точки доступа Wi-Fi, которая очень похожа на реальную. Когда пользователи подключаются по ней к интернету, злоумышленник получает личные данные: регистрационные сведения, информация о сетевом трафике. Попасться на такой вид мошенничества можно в местах, где беспроводная сеть, как правило, бесплатная:

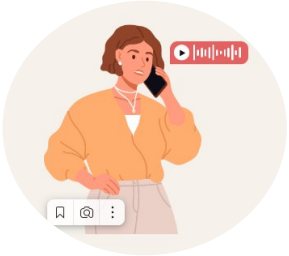
- аэропорт;
- кафе;
- библиотека;
- торговые центры;
- остановки общественного транспорта.

Фишинг в социальных сетях

Подразумевает использование социальных сетей, чтобы получить конфиденциальные данные жертв или заманить их нажать на определенные вредоносные ссылки. Хакеры могут создавать поддельные аккаунты, выдавая себя за кого-то из знакомых жертвы, чтобы заманить ее в свою ловушку, или они могут даже выдавать себя за аккаунт службы обслуживания клиентов известной компании, чтобы охотиться на жертв, которые обращаются в эту компанию за поддержкой.

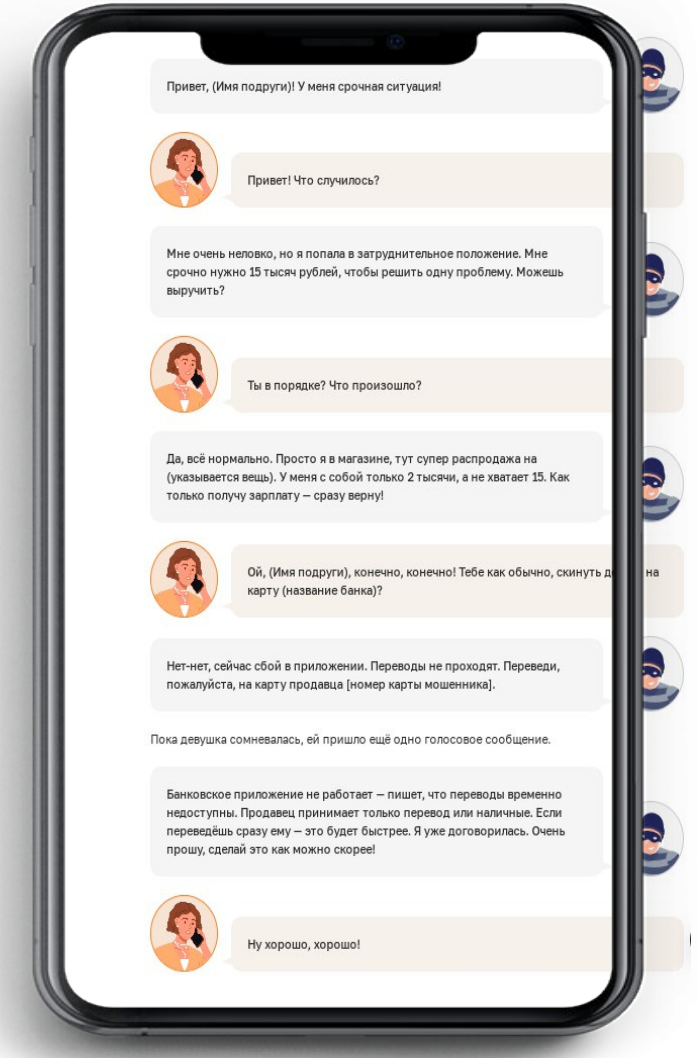


Злоумышленники использовали нейросеть, чтобы подделать голос подруги



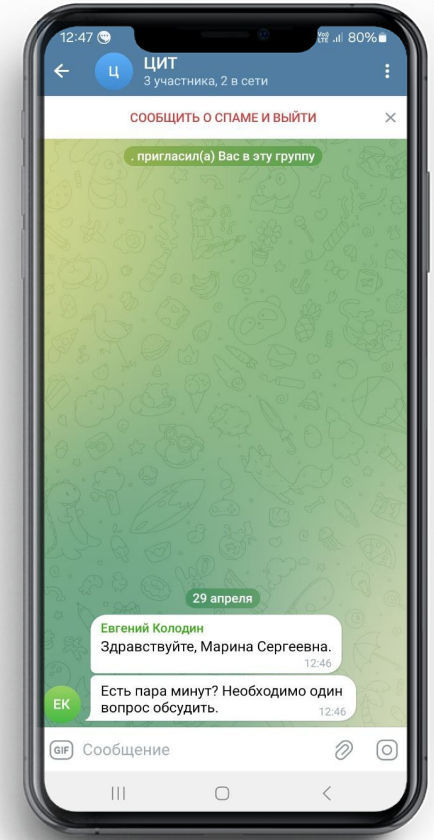
Две подруги дружили со школы — делились всем, ежедневно переписывались, присылали друг другу фотографии и обсуждали планы на выходные. Наша героиня была уверена, что она узнает голос своей подруги с первого слова. Но однажды это сыграло с ней злую шутку.

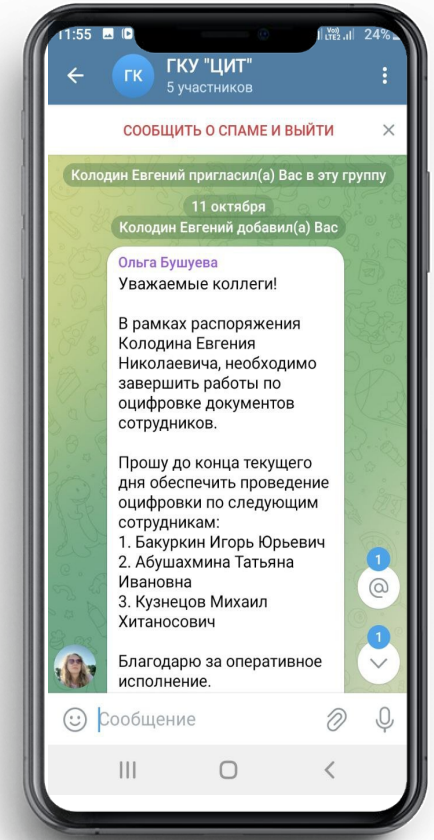
Спустя час девушка решила всё же позвонить подруге — и та была крайне удивлена. Оказалось, что её аккаунт в мессенджере взломали. Мошенники рассылали сообщения от её имени по всем контактам, прося деньги. Чтобы не вызывать подозрений, они использовали сгенерированные нейросетью голосовые сообщения, почти неотличимые от настоящего голоса подруги.



Создание фейковых акаунтов в социальных сетях

Сравнительно недавно в арсенале мошенников закрепилась новая схема, которая активно развивается. Злоумышленники не просто звонят или пишут вам от имени вашего начальства, но и даже создают от имени руководства организации «рабочие группы» в мессенджерах. Видя, что группа рабочая, и в ней присутствуют и другие коллеги, попасться на уловки мошенников





Вредоносное программное обеспечение

Это мошенничество, связанное с запуском вредоносного программного обеспечения на устройстве конечного пользователя.

Вредоносное ПО может быть внедрено в виде вложения в электронное письмо, загружаемого файла с сайта или путем использования известных уязвимостей в системе безопасности

После того как из Google Play и App Store удалили приложения крупных российских банков и компаний, подделок стало в разы больше: появились мошеннические копии RuStore и RuMarket, приложений Сбербанка и ВТБ.

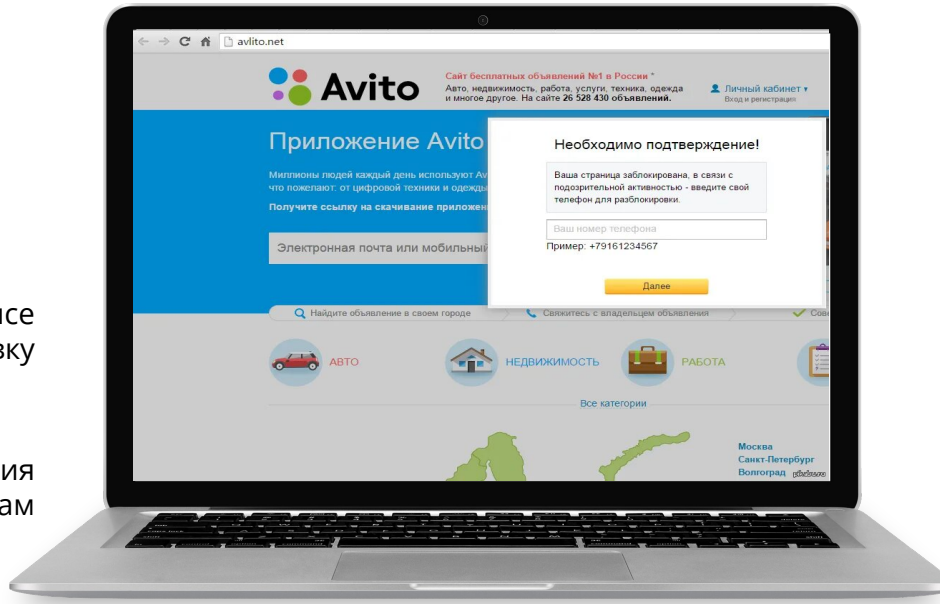
Некоторые приложения требуют предоставить им доступ к фотографиям или данным телефона. Хакеры сканируют устройство, находят чувствительные данные, а затем используют их для шантажа или взлома.

Веб-фишинг

Это мошенничество через поддельный сайт или , который ничем внешне не отличается от оригинала

Каким образом хакеры заводят пользователей на подобные сайты:

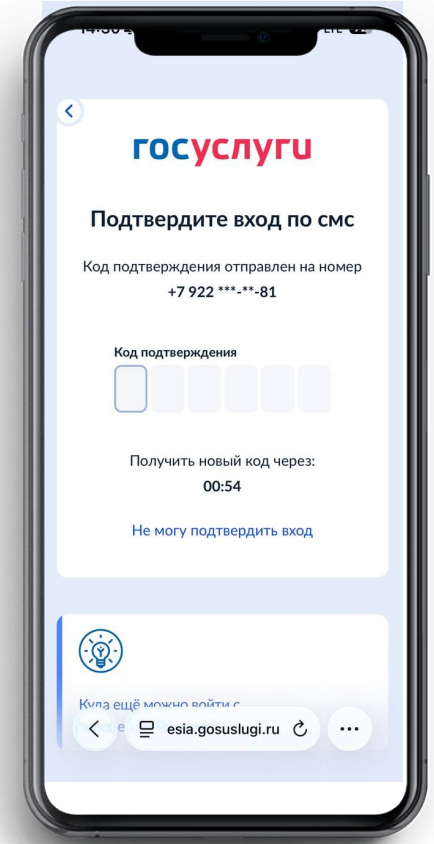
- Через поисковые системы.
- По целевой слежке за сотрудниками с последующей подменой страницы в рабочем письме.
- С помощью рассылки.



Например: Покупатель пишет продавцу на сервисе размещений объявлений “Авито”, что оплатить товар и доставку можно по ссылам: avito-dostavka-msk.ru, avito-deiiveri.ru.

По ссылке откроется фишинговый сайт — почти точная копия настоящего. С одним отличием: все данные, которые вы там введете, попадут в руки мошенникам.

госуслуги



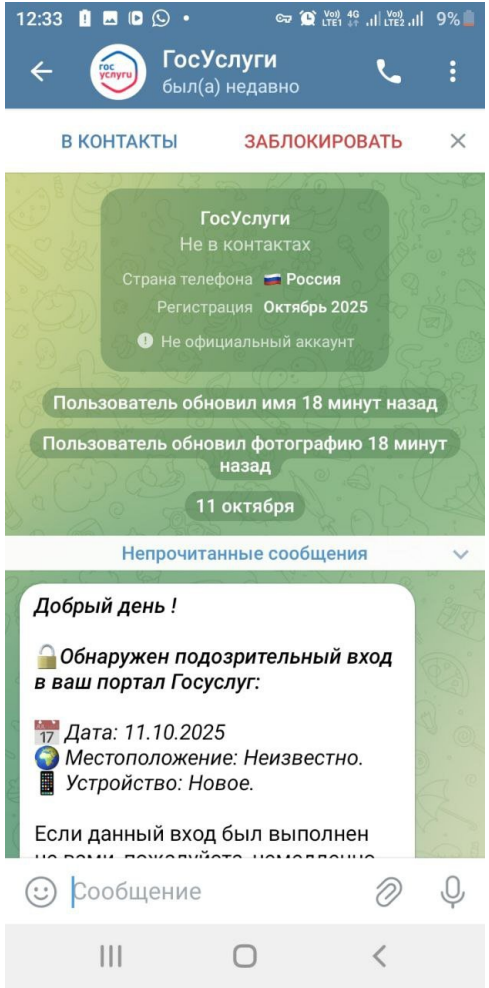
Доступ к «Госуслугам» россиян интересует мошенников из-за доступа к большому объему персональных сведений, которые хранятся в системе. Эта информация, включающая паспортные данные, ИНН, СНИЛС и банковские реквизиты, крайне ценный ресурс для совершения различных преступлений: от оформления кредитов на чужое имя и хищения денежных средств до мошенничества с недвижимостью, использованием чужой личности для получения государственных пособий или льгот.

Согласно данным от УМВД России по Оренбургской области в 2025 году доля мошеничеств, совершенных с использованием портала увеличилось на 35%.

Для получения доступа к личному кабинету достаточно знать код из СМС, который им сообщают граждане, находясь в состоянии заблуждения.

Как работают мошенники?!

1. **Создание паники.** Ване приходит сообщение в Telegram от аккаунта с аватаркой и синей галочкой. Указан официальный номер поддержки, но при звонке он перенаправляет к мошенникам.
2. **Звонок в техподдержку.** На линии «сотрудница Госуслуг»: спокойная, уверенная, но давящая на страх. Сообщает: «Вход в ваш аккаунт был из Киева».
3. **Ложная блокировка.** «Ваш аккаунт мы уже заблокировали, пока мошенники не получили доступ к данным». Человек расслабляется и начинает доверять.
4. **Код по СМС**. «Разблокировка возможна только через Центральный банк РФ. Пришлите код СМС». Ваня пересылает код, и доступ переходит к мошенникам.
5. **Вход и проверка данных.** Они сразу заходят в аккаунт, запрашивают список банков и кредитную историю.



Защита от фишинга

1. Проверяйте адрес отправителя.
2. Не переходите по ссылкам из писем.
3. Остерегайтесь срочных требований.
4. Не делитесь личной информацией.
5. Используйте антивирус.
6. Проверяйте ссылки перед переходом.
7. Будьте осторожны с вложениями.
8. Используйте двухфакторную аутентификацию.
9. Сообщайте о подозрительных письмах.

ВНИМАНИЕ!

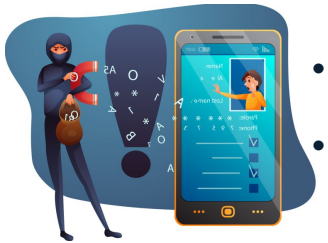
Письмо отправлено с внешнего адреса!

Если у вас **возникли сомнения** в достоверности отправителя,
не открывайте и не загружайте вложенные файлы!

Для проверки письма перешлите его на почтовый ящик:

checkme@mail.orb.ru

Как защитить телефон от действий мошенников?



- Включите автоматическую блокировку экрана.
- Закройте важные приложения и файлы паролем или отпечатком.
- Включите функцию поиска или удалённого управления. Установите программу или активируйте «Найти устройство».
- Скачивайте приложения только из официальных магазинов.
- Не переходите по подозрительным ссылкам.
- Установите антивирус из официальных магазинов и регулярно обновляйте его.
- Не давайте лишние разрешения приложениям.
- Обновляйте систему. Включите автоматические обновления, чтобы телефон был защищён.
- По возможности откажитесь от бесплатного WI-FI для важных действий.

Правила создания надежного пароля

• Не используйте один и тот же пароль для всех своих учетных записей.

• Забудьте о простых паролях.

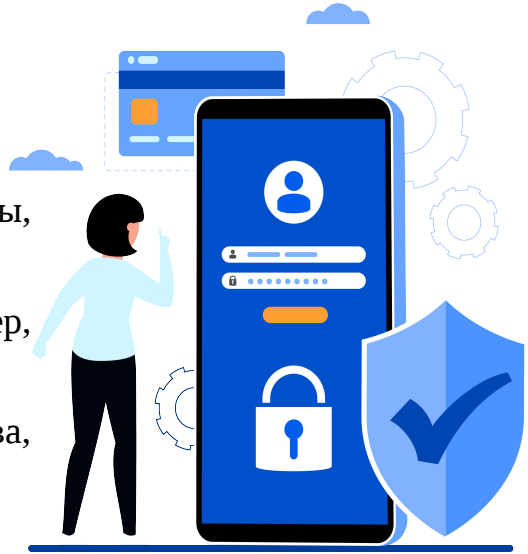
Длина пароля — 8–12 символов минимум.

• В пароле одновременно используются цифры, специальные символы, строчные и прописные буквы. Примеры специальных символов: #, %, *.

• В пароле отсутствуют популярные и простые сочетания. Например, последовательность цифр или букв: 123456, Qwerty.

• В пароле нет ваших личных данных. Например, имени, фамилии, отчества, даты рождения, серии или номера паспорта.

• Периодически обновляйте пароли.



Пример хорошего пароля: <tP0gfS_y0cN25!

*Этот пароль уже скомпрометирован, потому что его выложили в открытый доступ

Безопасность персональных данных

- Различные сервисы могут попросить подтвердить свою личность с помощью фотографии, где будут видны ваше лицо и паспорт. Когда вы делаете подобные снимки, свободными пальцами или второй рукой держите надпись с названием компании, в которую вы отправляете фотографию. Злоумышленники воруют такие снимки тысячами и им легче удалить вашу фотографию, чем пытаться стереть название компании.

- На сайтах с розыгрышами, выгодными инвестициями и другими способами быстро разбогатеть или получить что-то в подарок не нужно оставлять свои персональные данные. Ваши ФИО и номер телефона как минимум продадут черным маркетологам, а в 95% случаев мошенникам.

- Не выкладывайте фотографии и сканы документов, подтверждающих личность, в социальных сетях, даже в личных сообщениях.

Безопасный интернет

- В публичных местах, если вы подключились к бесплатному WiFi – **не вводите пароли** даже на известных и доверенных сайтах.
- **Не доверяйте всем QR-кодам**, которые видите. QR код- «от англ. QR - Quick Response - Быстрый Отклик» — это штрихкод, предоставляющий информацию для ее быстрого распознавания с помощью камеры на мобильном телефоне. Проверьте, не наклеен ли поверх одного кода другой.
- В социальных сетях и мессенджерах лучше **не открывать ссылки от незнакомцев**.
- Даже ваших знакомых могут взломать, так что, если они вам прислали ссылку без объяснения или с подозрительным объяснением, лучше ее **не открывать или проверить**, действительно ли это ваш знакомый.
- Если после перехода по подозрительной ссылке у вас запрашивают конфиденциальную или личную информацию, предлагают скачать файл – **уходите с сайта**.

Проверка скачиваемых файлов

- Всегда обращайте внимание на название расширения.
- Установите на устройство антивирус, который будет проверять все файлы на наличие угроз.
- В настройках мобильного устройства запретите установку из неизвестных источников.

Как обезопасить свою учётную запись

ГОСУСЛУГИ

Смс

Это наиболее простой, понятный и в то же время самый уязвимый способ защиты. Мошенники могут узнать код из смс у самого пользователя или настроить переадресацию его смс на свою сим-карту

Одноразовый код TOTP

Специальное приложение генерирует и каждые 30 секунд обновляет временный одноразовый код. Этот способ защиты надежён, так как одноразовый код генерируется только на вашем устройстве. Мошенники не смогут его узнать. Но вы не сможете войти на Госуслуги, если потеряете телефон или удалите приложение. Доступ придется восстанавливать в центре обслуживания или онлайн через банк

Биометрия

После ввода пароля камера ноутбука распознаёт ваше лицо и подтверждает вход. Войти на Госуслуги без вашего личного присутствия не получится — фотография не сработает. Но чтобы использовать этот способ, нужно зарегистрировать биометрию — стандартную или подтверждённую — и обновлять её каждые 3 года или 5 лет соответственно

Как обезопасить свою учётную запись

Как подключить уведомления о входе

1. Перейдите в личный кабинет → Профиль → Безопасность
2. Переведите переключатель «Уведомления о входе» в активное положение
3. Уведомления будут приходить на электронную почту, указанную в личном кабинете

> **Включите пуш-уведомления в приложении электронной почты**
>
> Это поможет вовремя отследить вход мошенников в вашу учётную запись на Госуслугах

Запрет на получение кредитов и займов

Как установить запрет

Порядок действий

1. Перейдите к услуге
2. Проверьте ваши данные: ФИО, серию и номер документа, удостоверяющего личность, ИНН
3. Выберите, какой вид запрета хотите установить: полный или частичный
4. Проверьте сформированное заявление и подпишите его любой электронной подписью
5. Отправьте заявление. Его рассмотрят в течение 2 календарных дней

Уведомления об установлении запрета придут от 4 квалифицированных бюро кредитных историй (КБКИ) в личный кабинет. Дата, с которой начнёт действовать запрет, будет указана во вложении

> КБКИ не могут отказать в предоставлении услуги. Услуга бесплатная

Запрет устанавливается бессрочно, и в любой момент его можно снять

Как снять запрет

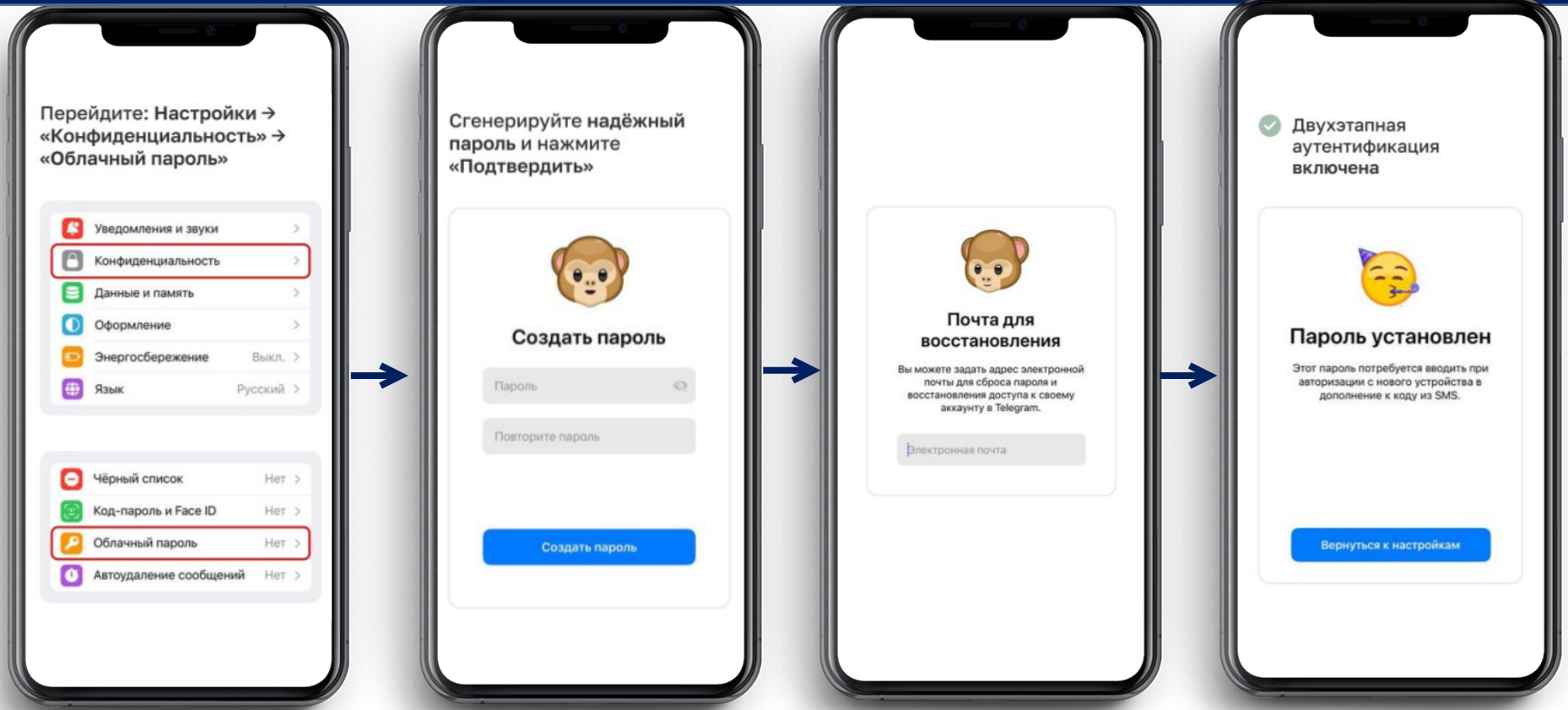
Снять запрет можно в любое время. Снимать запрет и устанавливать его повторно можно неограниченное количество раз

Порядок действий

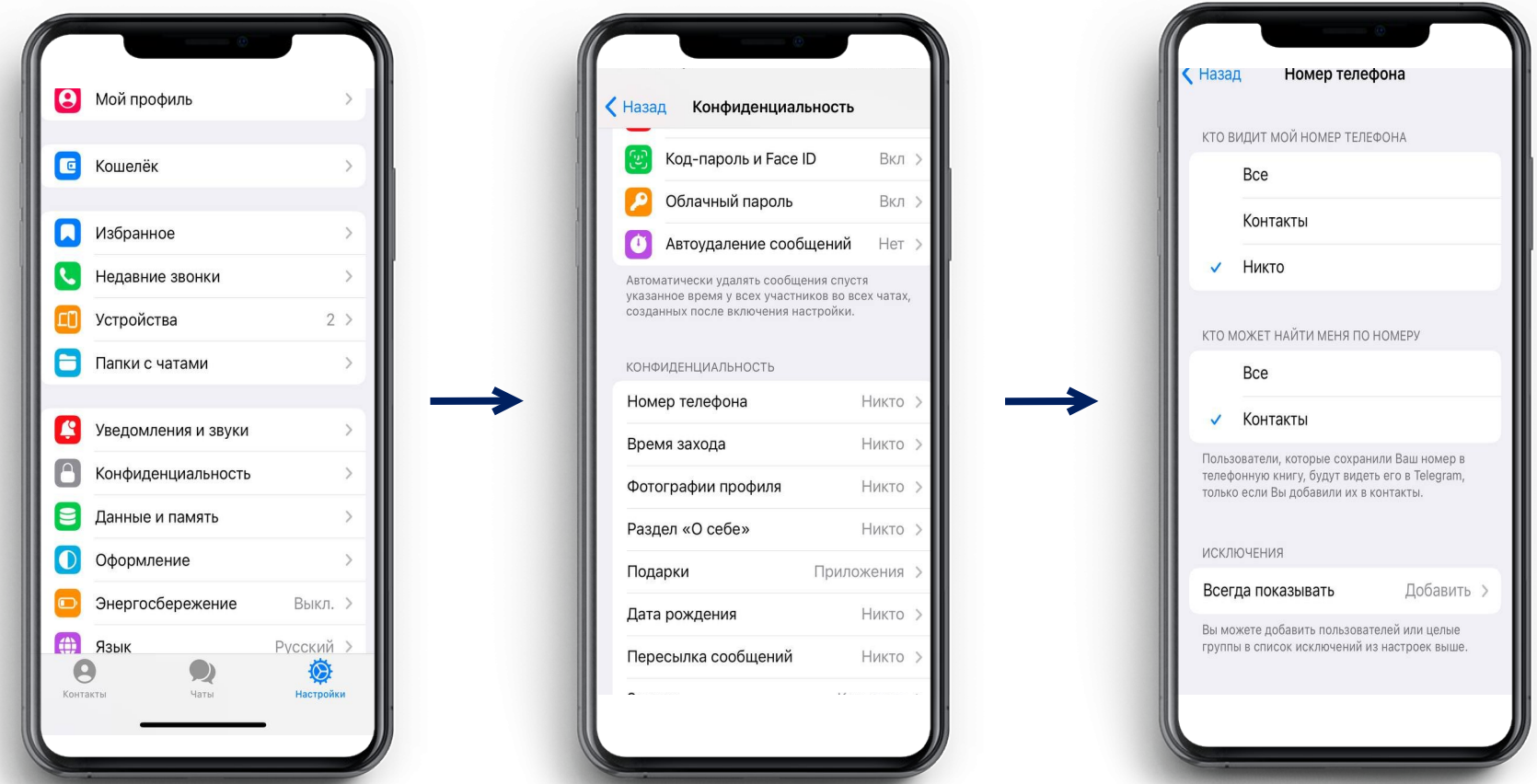
1. Перейдите к услуге
2. Проверьте ваши данные: ФИО, серию и номер документа, удостоверяющего личность, ИНН
3. Подпишите заявление электронной подписью. Для этого потребуется приложение «Госключ» или усиленная квалифицированная электронная подпись (УКЭП)
4. Отправьте заявление. Его рассмотрят в течение 2 рабочих дней

Запрет будет снят только после того, как придут уведомления от всех 4 КБКИ в личный кабинет

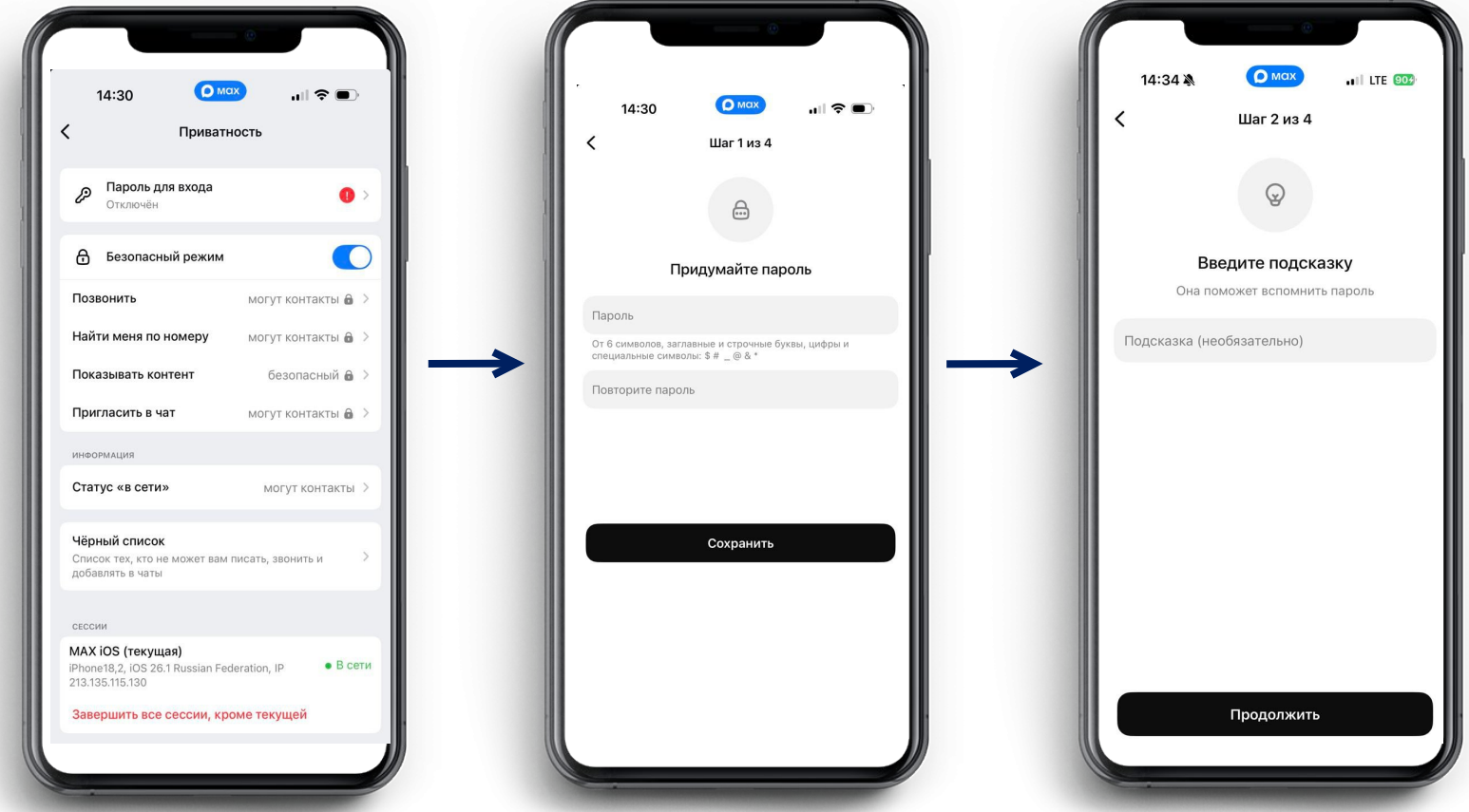
Настройка облачного пароля в Telegram



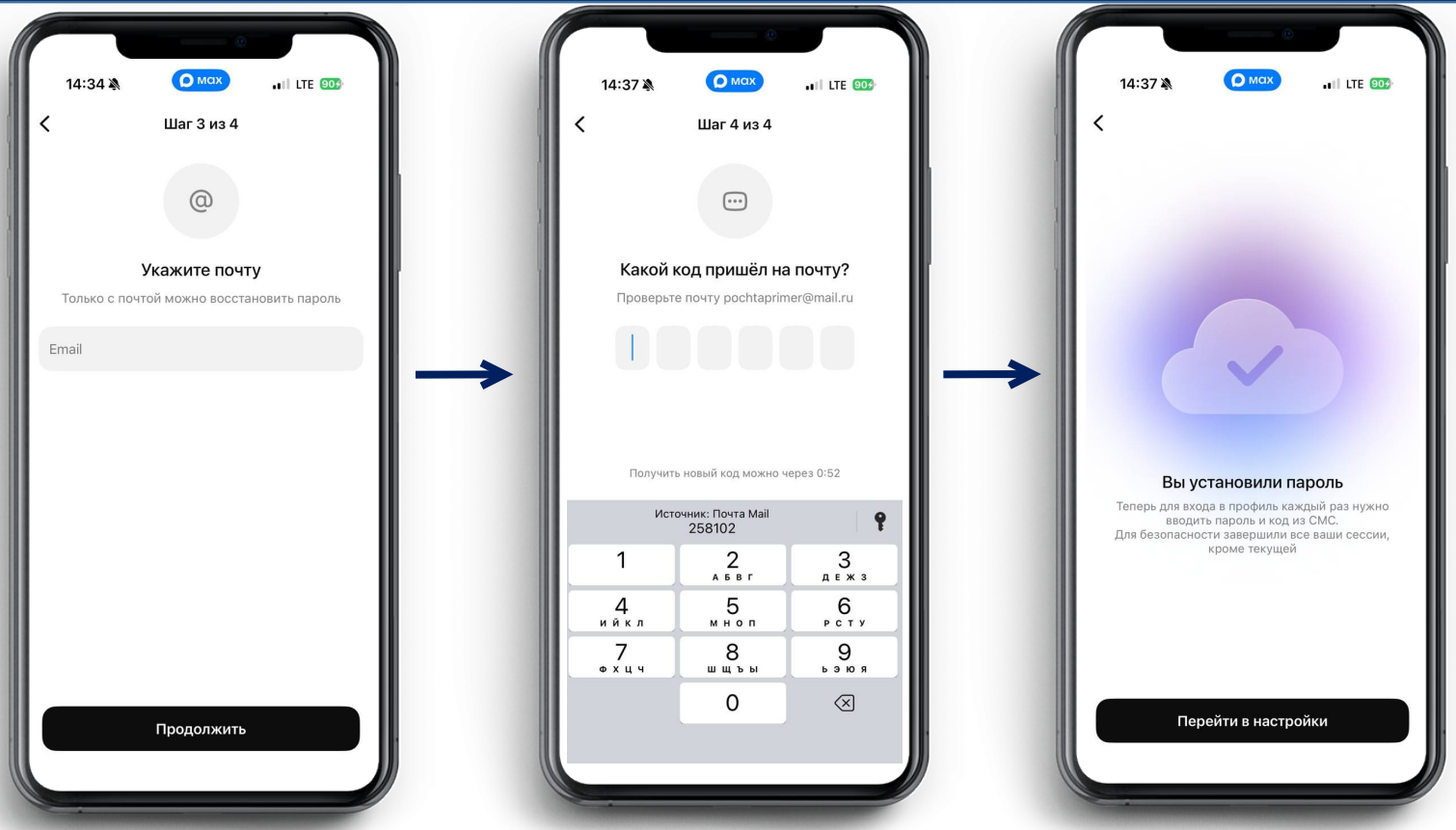
Настройка конфиденциальности в Telegram



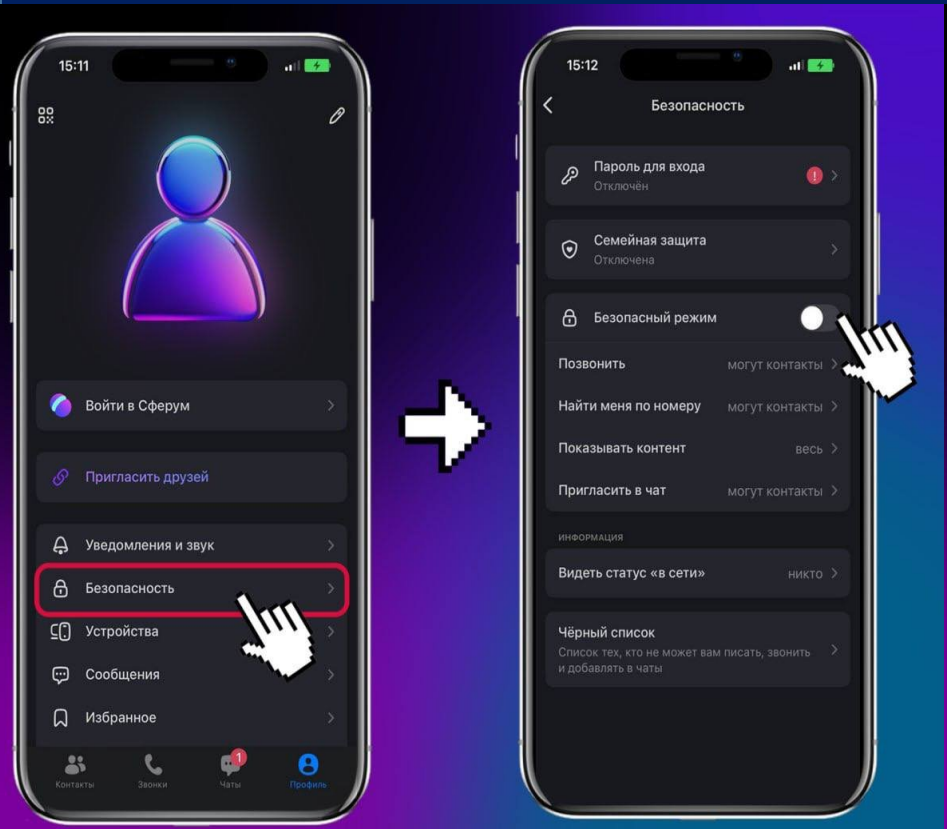
Как включить двухфакторную аутентификацию в MAX

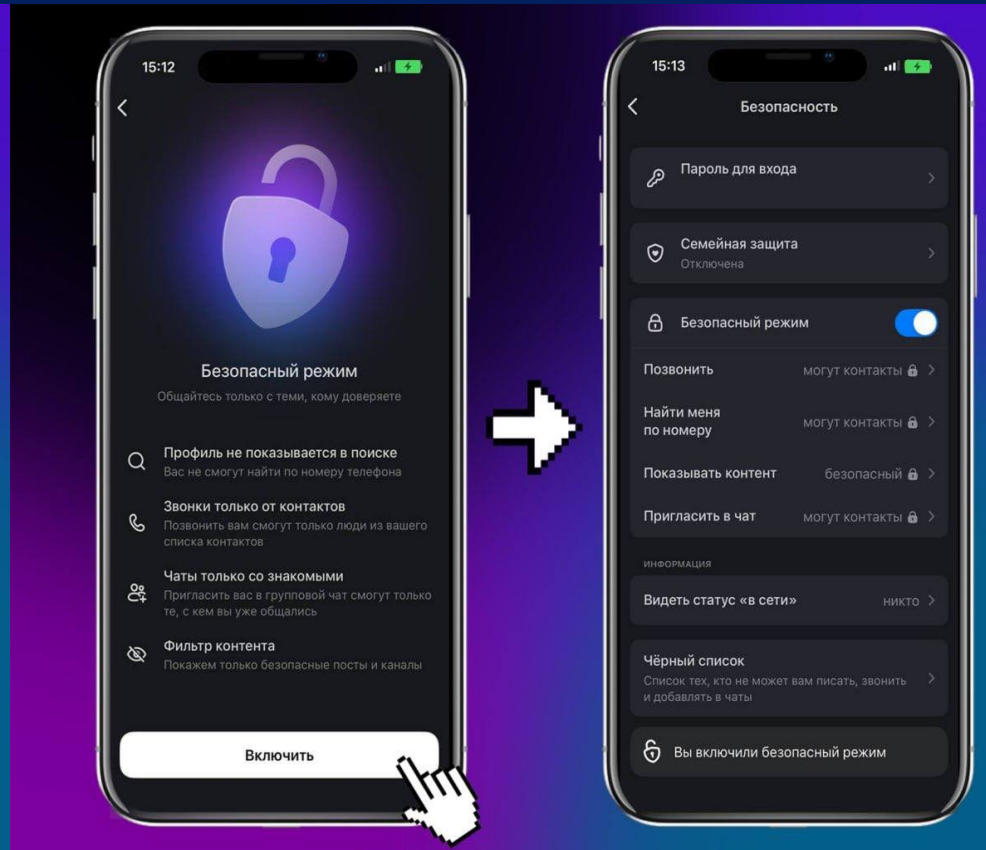


Как включить двухфакторную аутентификацию в MAX

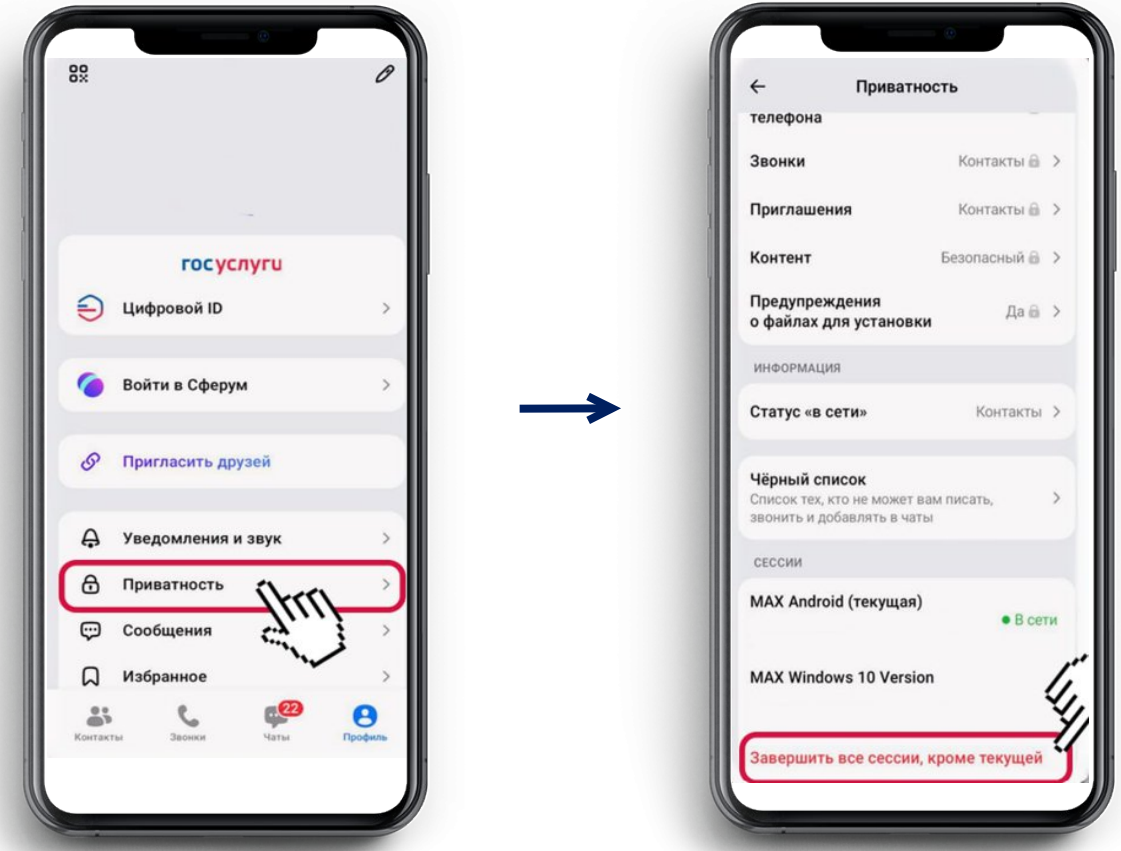


Настройка конфиденциальности в MAX

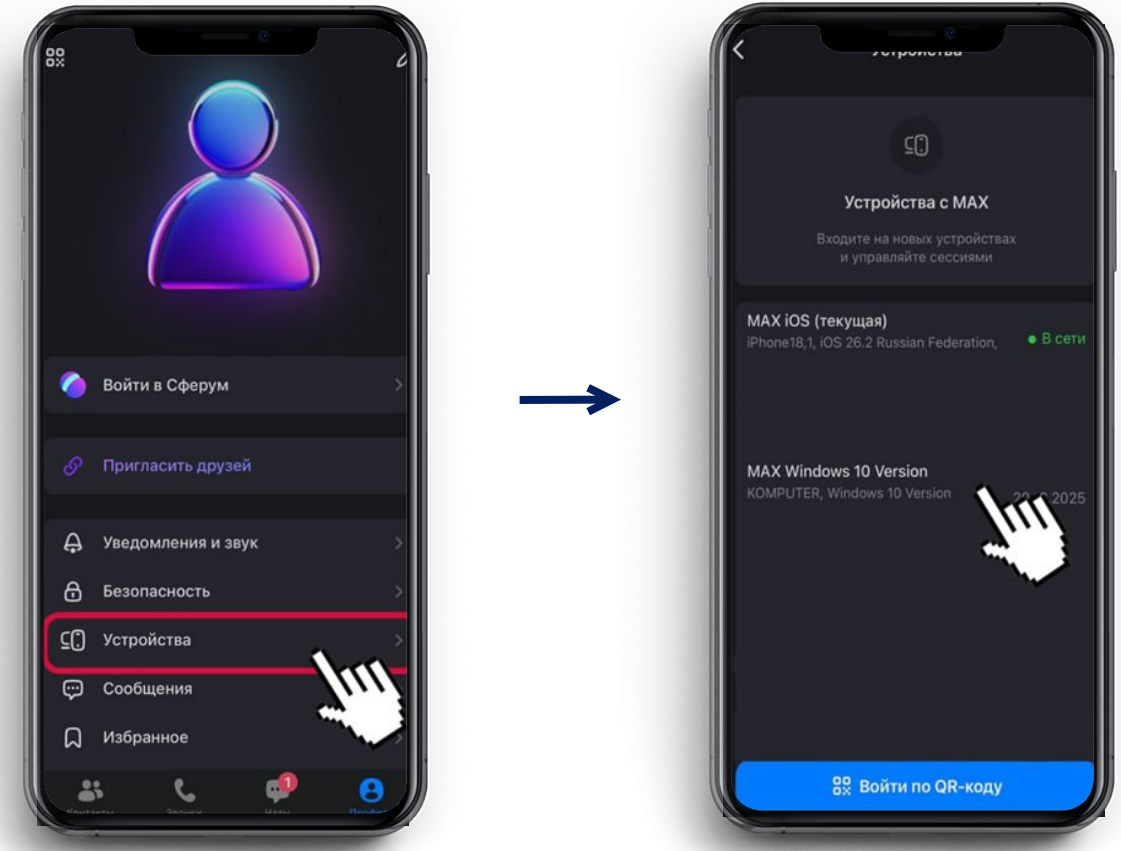




Контроль сессий в MAX (Android)



Контроль сессий в MAX (*IOS*)



Куда обратиться, если вы стали или предполагаете, что стали жертвой мошенничества?

!

Оставьте заявление о действиях мошенников:

- По телефону горячей линии МВД 8 800 222-74-47;
- По телефонам **02** (со стационарных телефонов) и **102** (с мобильных средств связи);
- На сайте МВД;
- В отделении полиции по месту жительства;

Будьте бдительны и осторожны!