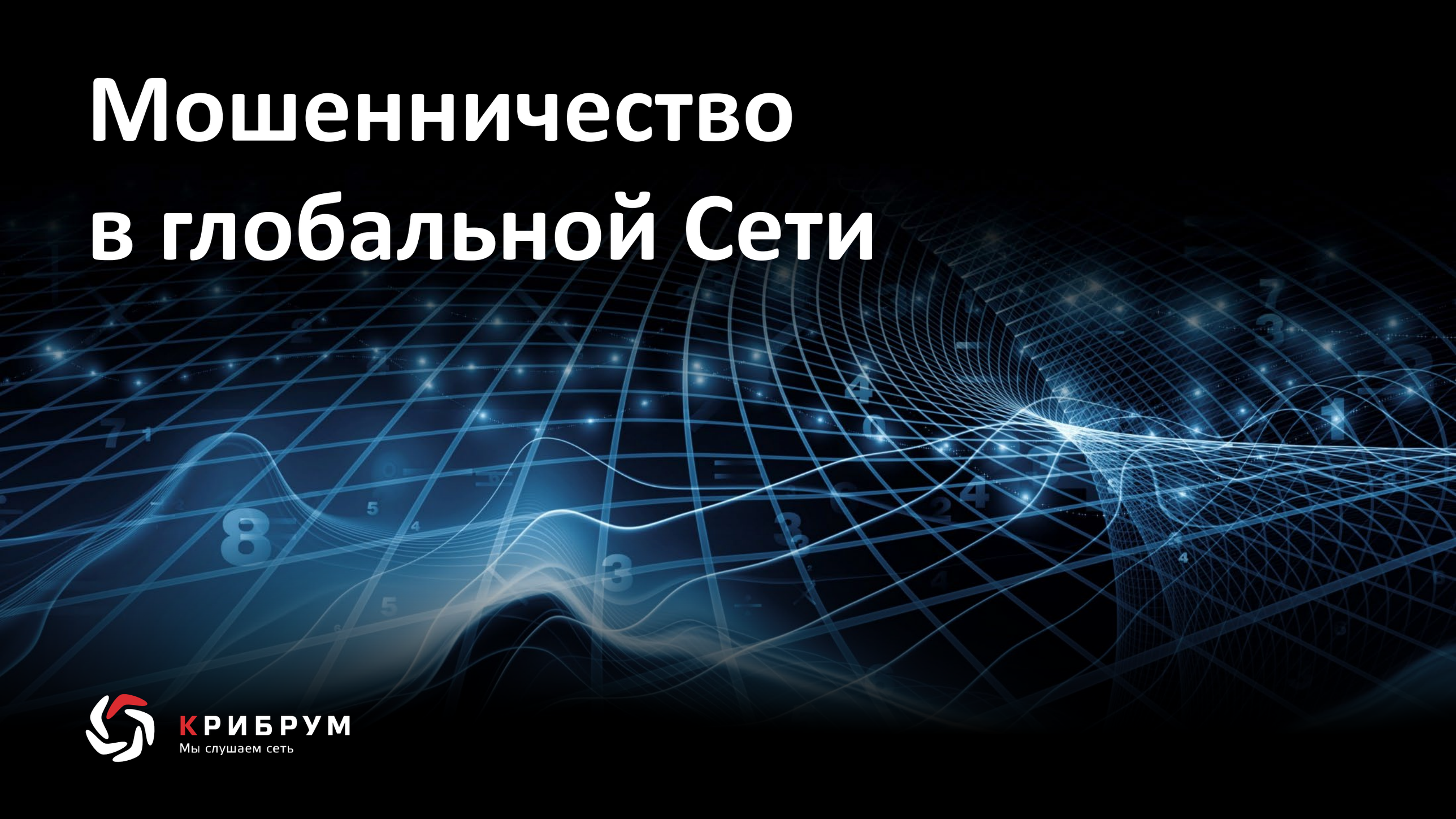
Мошенничество в глобальной Сети



КРИБРУМ
Мы слушаем сеть

Виды мошенничества, связанные с общением через мессенджеры

КРИБРУМ
Мы слушаем сеть

Мошенничество через мессенджеры

КРИБРУМ
Мы слушаем сеть

Мошенничество, при котором злоумышленники используют чужие профили в социальных сетях или мессенджерах, известно как «клонирование профиля» или «фейковый профиль». Это типичный метод мошенничества, который может иметь различные цели, включая обман и вымогательство, но в большинстве случаев основной целью является получение материальной выгоды.

Вот некоторые типичные сценарии такого мошенничества:

фейковые профили;

поддельные истории;

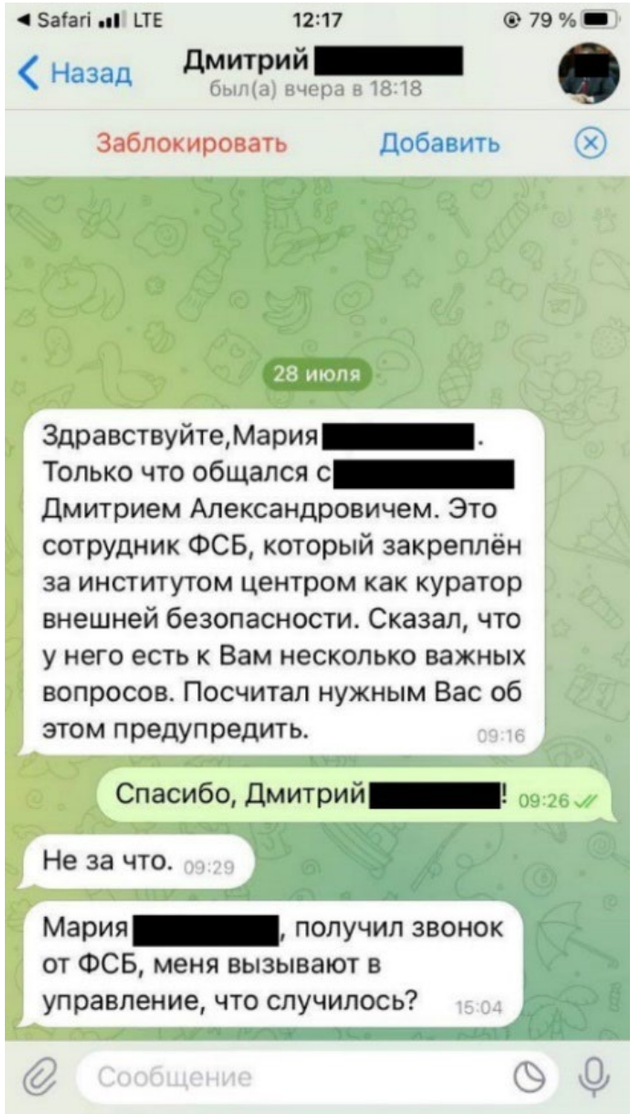
фишинг «под маской» известных организаций.

Фейковые профили

КРИБРУМ
Мы слушаем сеть

Мошенники создают фейковые профили, используя фотографии других людей, чтобы притвориться этими людьми.

Они могут использовать имена и фотографии, которые найдут онлайн или украдут с других аккаунтов. Такой способ распространен в Telegram. Профиль имеет скрытый номер. Звонки осуществляются через сам мессенджер с подменного номера (номера могут быть как мобильные, так и городские и принадлежать структурам в зависимости от легенды).

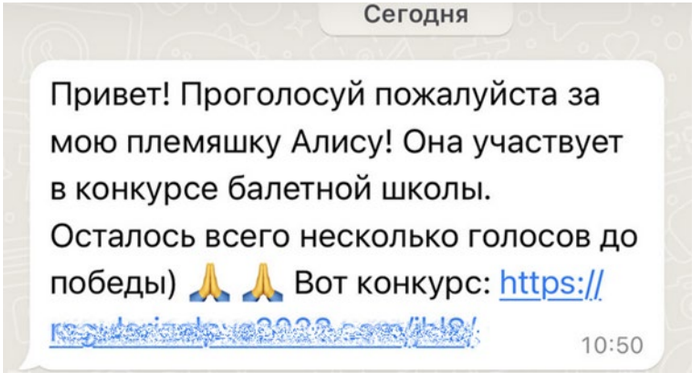


Мошенничество с помощью поддельных историй

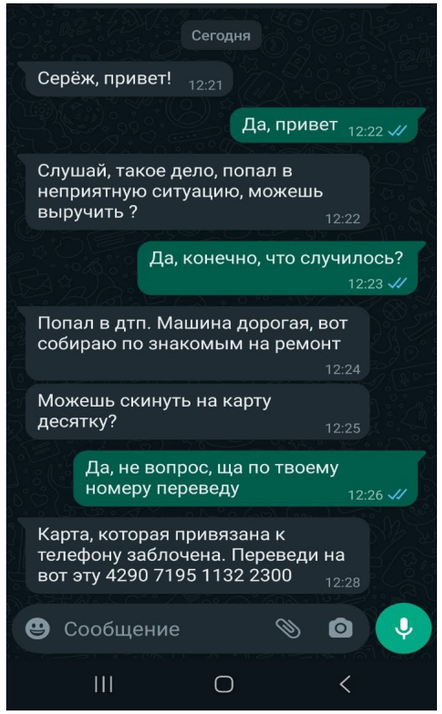
КРИБРУМ
Мы слушаем сеть

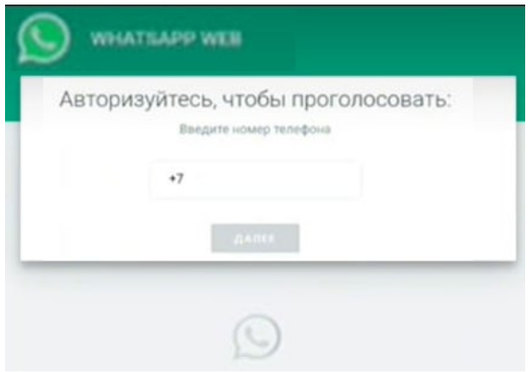
Мошенники также могут притворяться жертвами бедствий, просить пожертвования или помощь, использовать сочувствие пользователей в своих интересах

Мошенники могут устанавливать отношения с людьми через социальные сети, представляясь кем-то другим, затем запрашивать деньги или личную информацию под разными предлогами. Особую опасность представляет тот момент, когда злоумышленники получают данные от аккаунтов различных пользователей и создают от их имени поддельную историю.



В последнее время основной оборот подобных мошеннических действий происходит в WhatsApp. В мессенджере можно подключить к одной учетной записи несколько устройств. Мошенники, получив доступ к устройству (вероятные способы получения доступа могут быть различные), отправляют сообщения контактам от вашего имени, которые вскоре удаляются на вашем гаджете. Текст сообщений может быть разный, но основной акцент направлен на то, чтобы пользователь перешел по ссылке.





После перехода устройство может быть заражено вирусом, который будет отслеживать ваши личные данные (например, банковские карты). Но в основном при переходе по подобным ссылкам происходит перенаправление на фишинговые сайты, где действительно может проводиться какое-то голосование, но при попытке оставить голос система попросит вас авторизоваться. Получив доступ к контактам абонентов и WhatsApp, злоумышленник осуществляет рассылку от вашего имени для получения материальной выгоды (перевести деньги, сообщить код из смс и т. д.).

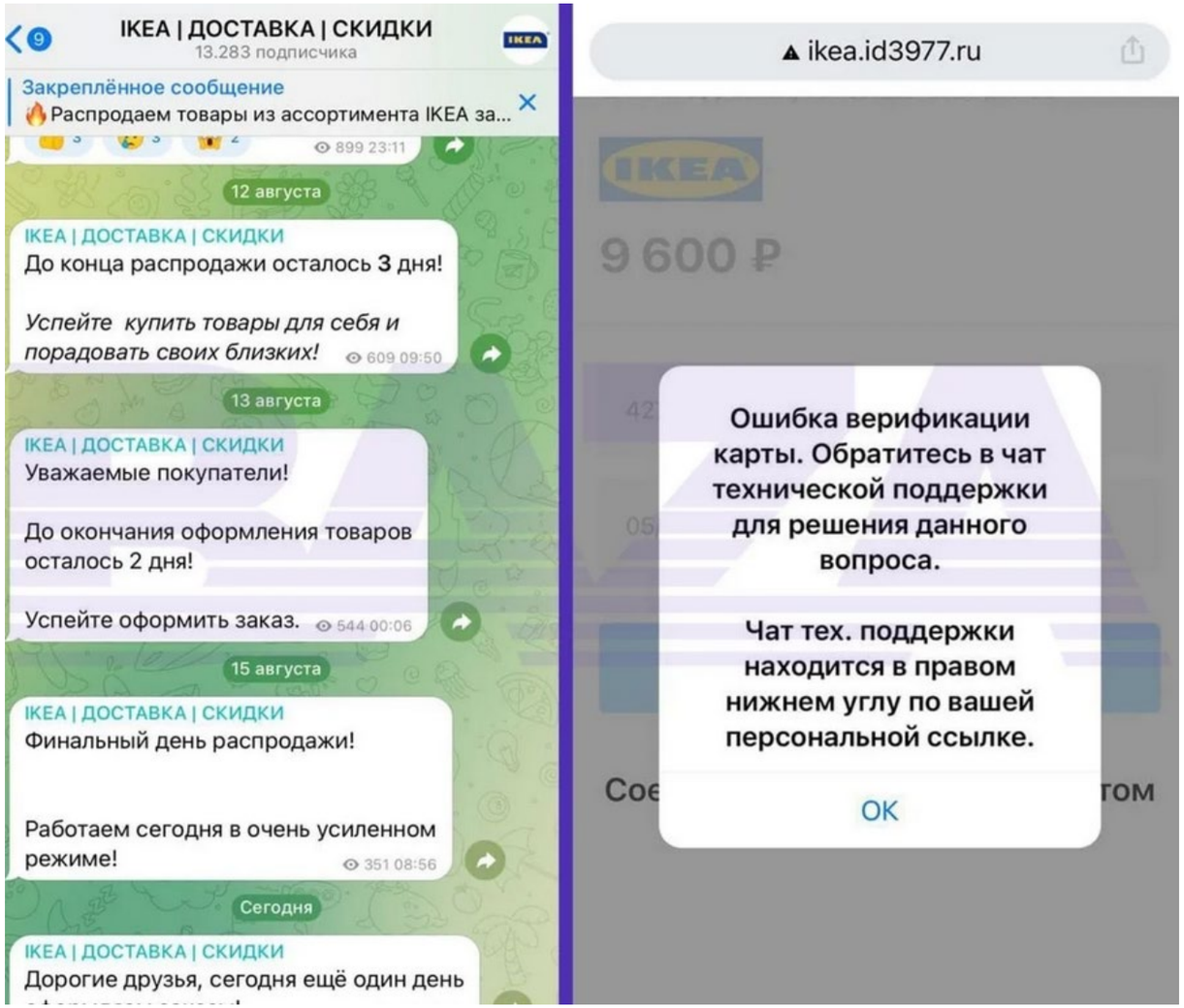
Подобные схемы могут происходить и с другими аккаунтами в социальных сетях.

Фишинг с использованием известных организаций и брендов

КРИБРУМ
Мы слушаем сеть

Мошенники могут использовать фейковые аккаунты, чтобы отправлять сообщения якобы от официальных источников. Такие сообщения содержат просьбы предоставить личные данные или пароли.

Оригинальный сайт	Фишинговый сайт
ikea.com/ru/ru/	▲ ikea.id3977.ru
✓	X

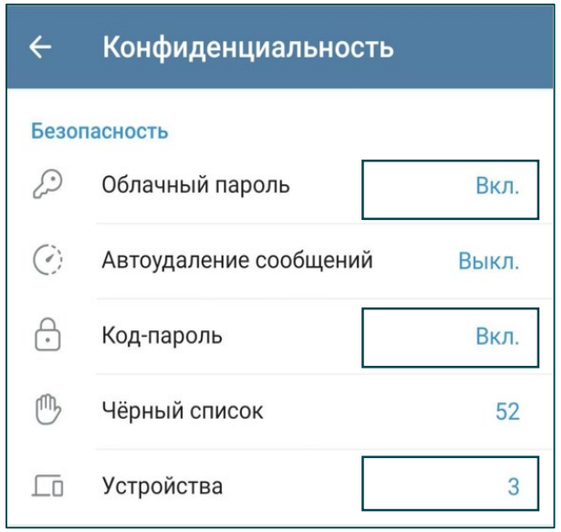


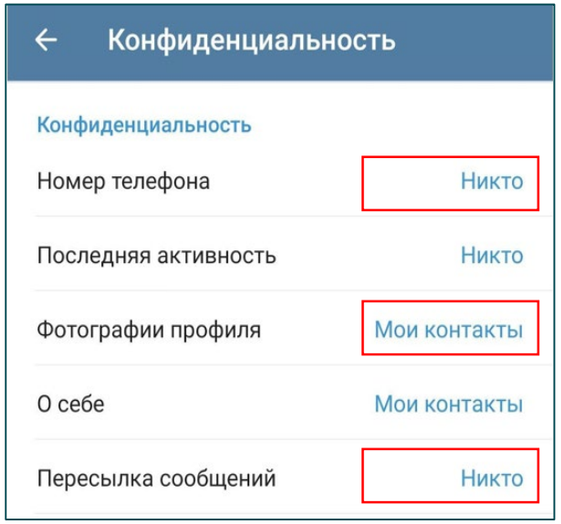
Защита Telegram-аккаунта

КРИБРУМ
Мы слушаем сеть

Для оптимальной защиты необходимо поменять настройки аккаунта

1. **Включите функцию облачного пароля в настройках конфиденциальности.** Это ограничит злоумышленнику возможность подключения новых устройств, даже если у него есть доступ к вашей сим-карте.
   Также облачный пароль поможет защитить ваш аккаунт при реализации атаки на веб-версию приложения.
2. **Подключите функцию «Код-пароль».** Это ограничит доступ к сообщениям, если ваше устройство оказалось в руках злоумышленника.
3. **В настройках следует скрыть номер телефона, выставив опцию «Никто». Также** лучше скрыть фото на аватаре, оставив его видимым только для контактов. Следует ограничить возможности по приглашению в группы и каналы, пересылке ваших сообщений и пр.
4. **Регулярно проверяйте в настройках телефона открытые сеансы с неизвестных устройств.**





Общаясь, не выполняйте просьбы незнакомцев, не переходите в видео-чат, где вас попросят показать свой экран, не присылайте скрины, не отправляйте никаких папок из Telegram.

Не вступайте в сомнительные группы: ваш аккаунт может быть сохранен в списки для рассылки спам-сообщений.

Следует помнить, что при вступлении в «чувствительные» группы (с политическим содержанием, дейтинговые и др.) информация о дате вступления, дате выхода, а также все сообщения с высокой степенью вероятности будут сохранены сервисами мониторинга.

Оптимально, если Telegram-аккаунт привязан к номеру, не зарегистрированному на паспортные данные пользователя.

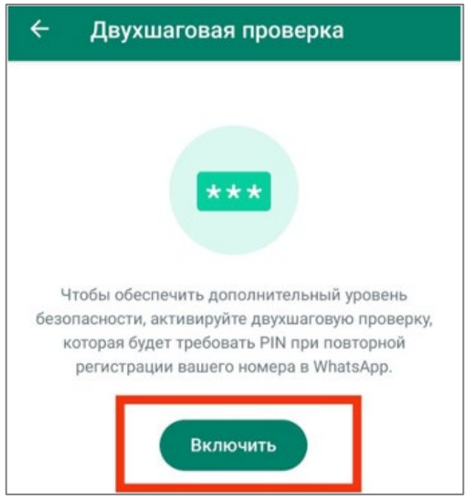
Защита WhatsApp от взлома

КРИБРУМ
Мы слушаем сеть

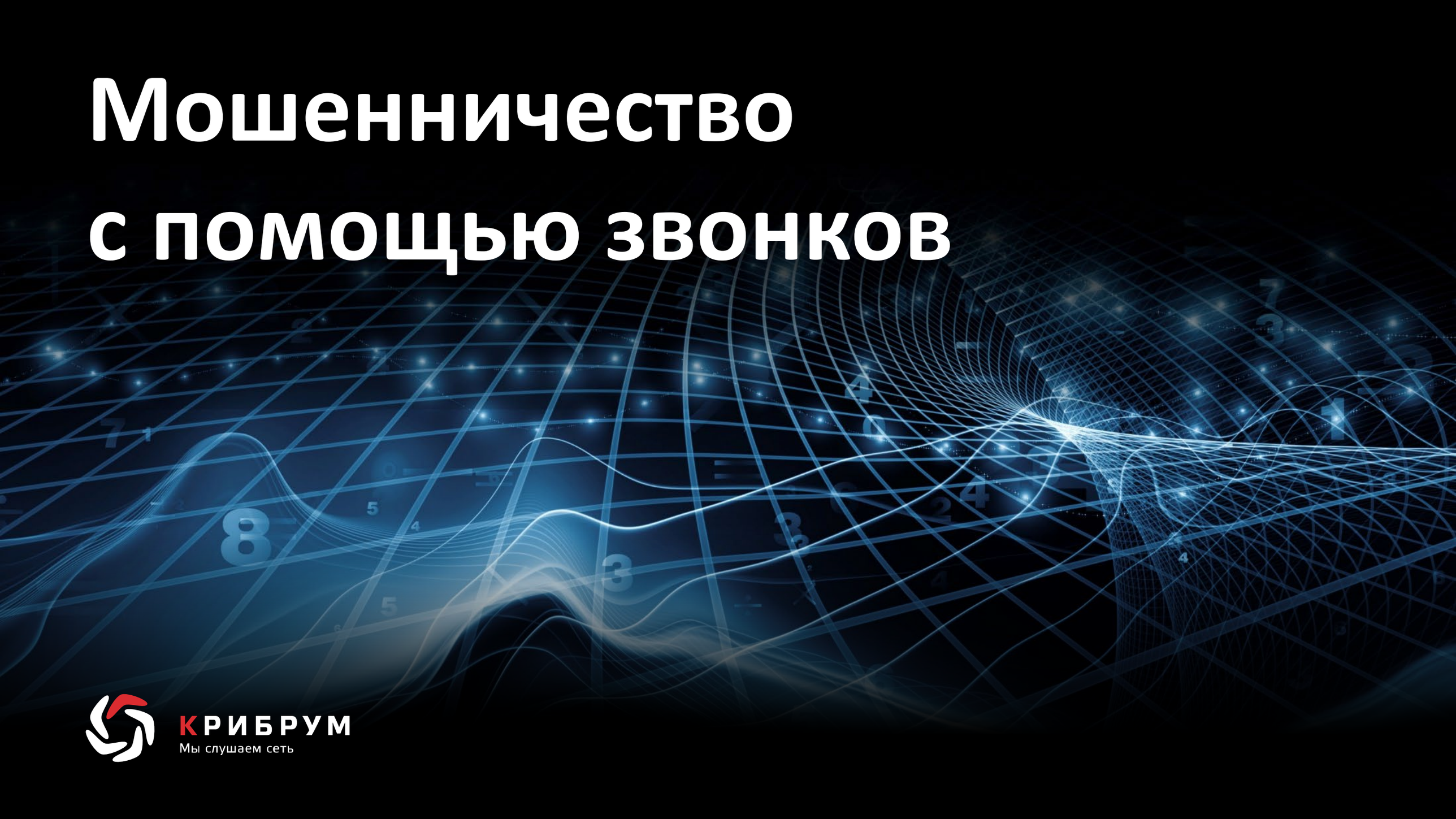
Для защиты вашего смартфона от взлома в приложении WhatsApp в первую очередь необходимо включить двухфакторную аутентификацию.

Для этого нажимаем на три точки в верхнем правом углу, выбираем «Настройки», переходим в меню «Аккаунт», нажимаем вкладку «Двухшаговая проверка», активируем ее нажатием кнопки «Включить», придумываем шестизначный пин-код.

WhatsApp также позволяет подключиться к своему аккаунту со стационарного компьютера, ноутбука или другого смартфона через QR-код или номер. Если в процессе пользования смартфоном были случаи оставления его без присмотра в разблокированном состоянии или вы прошли верификацию на фишинговом сайте, то необходимо проверить подключение чужих «связанных устройств», при обнаружении подозрительных - отключить их. Для этого выбираем вкладку «Чаты», нажимаем на три точки в верхнем правом углу, выбираем пункт «Связанные устройства». При наличии неизвестных устройств, отвяжите их.



Мошенничество с помощью звонков



КРИБРУМ
Мы слушаем сеть

Мошенничество с помощью звонков

КРИБРУМ
Мы слушаем сеть

Мошенничество с помощью звонков (телефонное мошенничество) - это вид правонарушений, при которых злоумышленники используют телефонные звонки. Вот несколько распространенных видов мошенничества с использованием звонков:

1. **мошенничество «по старинке»:** злоумышленники могут представляться сотрудниками банков, правительственных организаций, компаний, запрашивать личную информацию, такую как номера кредитных карт;
2. **мошенничество с помощью робоколлов:** злоумышленники могут использовать автоматические маркетинговые звонки для распространения мошеннических предложений, например, предлагая фиктивные продукты или услуги;
3. **мошенничество через поддельные номера**: злоумышленники могут подделывать номера телефонов, чтобы казаться более надежными, могут использовать номера известных организаций или банков;
4. **мошенничество с угрозами**: мошенники могут угрожать судебными исками, арестом или другими негативными последствиями;

Методы борьбы

КРИБРУМ
Мы слушаем сеть

Борьба с телефонным мошенничеством требует предупреждения, осторожности и использования доступных инструментов и технологий. Вот несколько способов борьбы с этим видом мошенничества:

1. **не предоставляйте личную информацию.** Никогда не предоставляйте личные данные (о банковских картах, счетах и вкладах, паспортные данные, коды и уведомления из электронной почты и СМС и т. д.). Будьте бдительны с поддельными номерами. Злоумышленники могут подделывать номера телефонов, делая их похожими на номера известных организаций**. ПОМНИТЕ! Ни одна официальная банковская или государственная организация не запрашивает данные банковских карт, коды из SMS-сообщений и т. д.;**

2. **не взаимодействуйте с автоматическими робоколлами.** Просто положите трубку. Мошенники могут использовать ваши ответы для определения активных номеров;

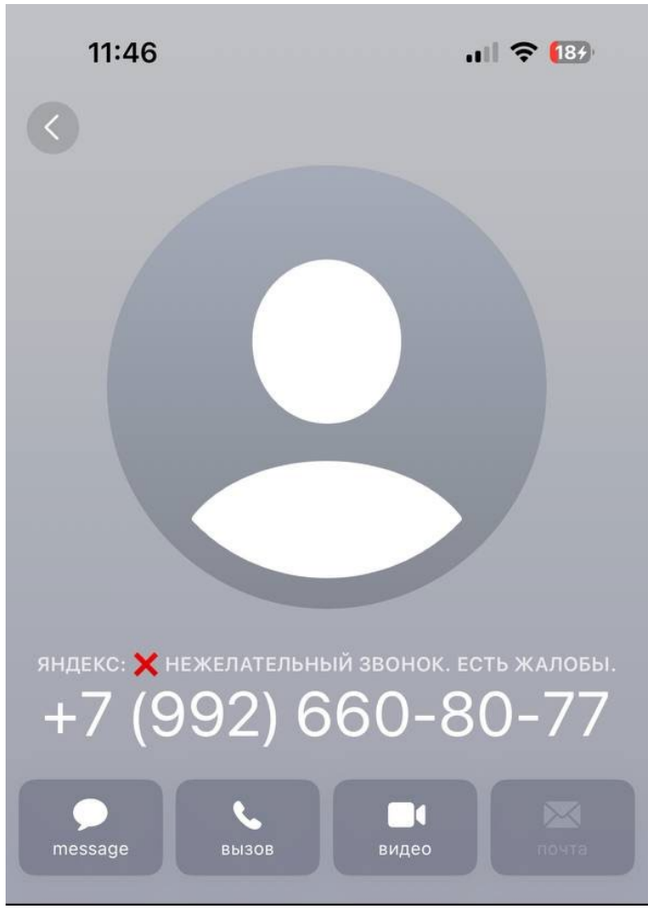
3. **установите программное обеспечение для блокировки звонков.** Многие мобильные приложения и операторы связи предоставляют функции блокировки нежелательных звонков и SMS. Используйте их, чтобы отфильтровать спам и мошеннические звонки;

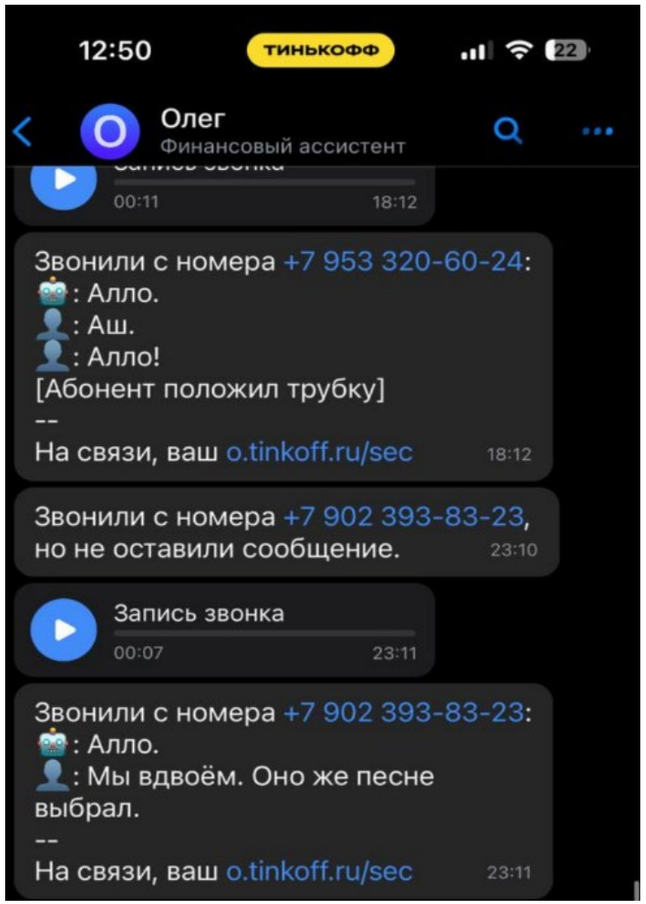
4. **обучение и информирование.** Образовывайте себя и других о распространенных мошеннических схемах. В глобальной сети огромное количество статей, как обезопасить себя от мошенников. Если вы стали жертвой мошенничества или получили подозрительный звонок, сообщите об этом местным правоохранительным органам и своему оператору мобильной связи.

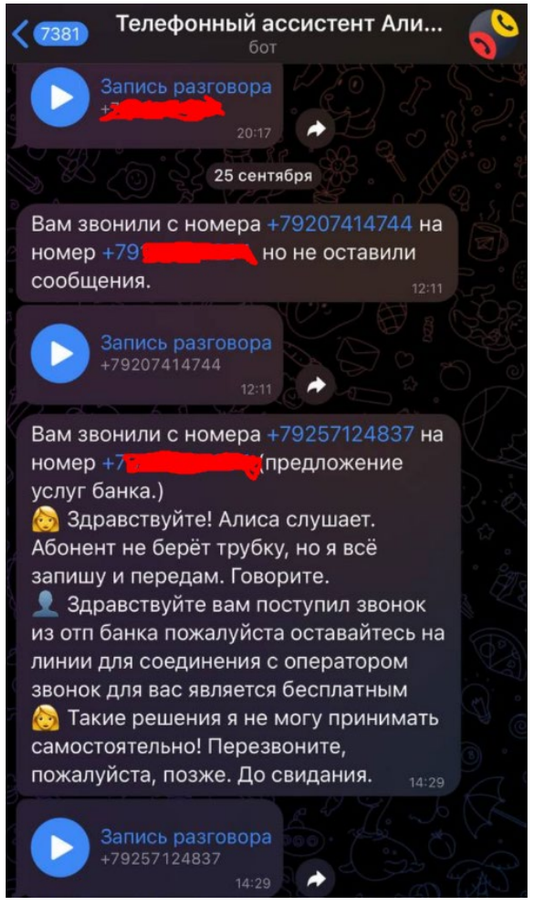
Методы борьбы

КРИБРУМ
Мы слушаем сеть

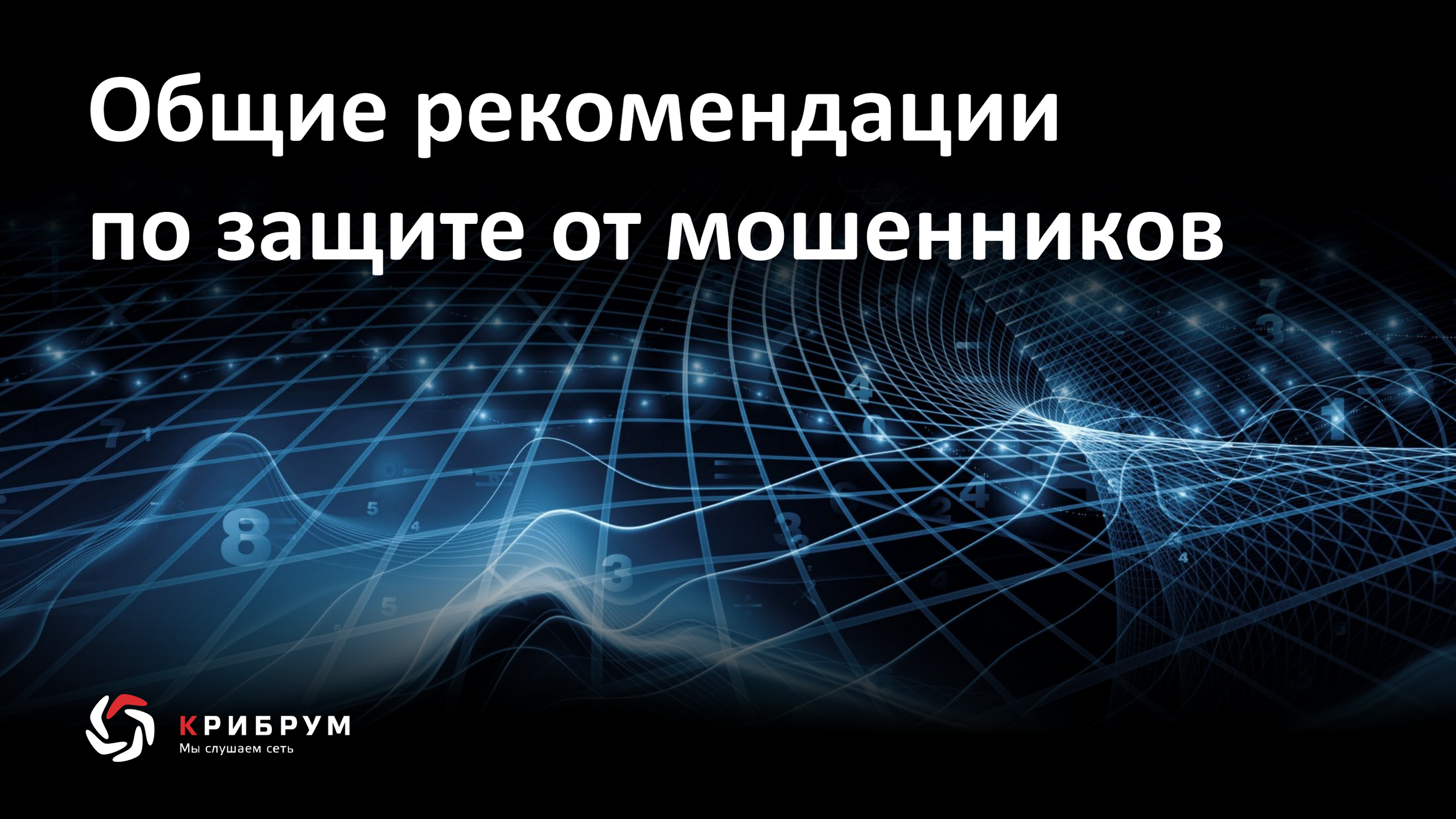
Защититься от мошеннических звонков помогают сервисы и приложения «Яндекса» («Алиса»), операторов связи («Ева» от «Мегафона») и крупных российских банков (робот «Олег» от «Тинькофф») и т. д.







Общие рекомендации по защите от мошенников



КРИБРУМ
Мы слушаем сеть

Общие рекомендации по защите от мошенников

КРИБРУМ
Мы слушаем сеть

Существует множество видов мошенничества в Интернете, способы защиты могут различаться. Рассмотрим самые распространенные виды мошенничества и перечислим некоторые способы, чтобы обезопасить себя:

1. **Мошенничество с банковскими данными**
   - Периодически проверяйте банковские выписки и кредитные отчеты на наличие подозрительных транзакций.
   - Используйте сложные пароли для банковских аккаунтов, дополнительно подключите двухфакторную аутентификацию (2FA).
2. **Социальная инженерия**
   - Будьте осторожны с информацией, которую вы публикуете в социальных сетях, — мошенники могут использовать ее для психологических атак.
   - Если кто-то пытается получить от вас личную информацию (ваши персональные данные или персональные данные других людей), убедитесь, что это не мошенники. Предупредите человека, о котором пытались получить информацию.
3. **Мошенничество при онлайн-покупках**
   - Оплачивайте товары и услуги только с надежных и проверенных сайтов.
   - Проверяйте отзывы о продавце, убедитесь, что он предоставляет контактную информацию.
   - Будьте осторожны с неожиданными предложениями или «подарками». Не доверяйте запросам на предоставление личной информации или оплату.
   - Внимательно проверяйте URL-адреса веб-сайтов, удостоверьтесь, что вы находитесь на официальном сайте компании, организации, социальной сети и т. п.
4. **Программы-вымогатели (Ransomware)**
   - Создавайте резервные копии важных данных, чтобы иметь возможность их восстановить без уплаты выкупа в случае атаки программы-вымогателя.
   - Используйте лицензированное антивирусное программное обеспечение и избегайте скачивания неизвестных файлов.
   - Загружайте приложения только из официальных магазинов.
   - Проверяйте отзывы и рейтинги приложений перед их установкой.

Общие рекомендации по защите от мошенников

КРИБРУМ
Мы слушаем сеть

Необходимо помнить, что мошеннические схемы основаны на спекуляции нашими страхами и пороками. В основе сценария мошенников всегда лежит предсказуемость человеческого поведения в стрессовых ситуациях. Мошенники сначала нагнетают эмоциональное напряжение, вызывают чувство тревоги, провоцируют чрезмерное возбуждение. Человек начинает испытывать потребность совершить какие-либо действия. В этот момент мошенник как бы предлагает помощь, выступает в качестве опоры в критической ситуации, внушает, что нужно сделать, чтобы спасти себя от проблем с законом или избежать потери денежных средств. Порог критичности снижается, возникает неосознанное доверие к собеседнику.

Что следует делать:

- соблюдать эмоциональную дистанцию с мошенниками, не терять самоконтроль;
- критически оценивать ситуацию и задавать себе вопросы: «для чего я собираюсь совершить это действие?», «что они получат, если я так поступлю?»;
- вести себя вопреки ожидаемым реакциям: отберите инициативу у мошенников, задавайте вопросы, которые не вписываются в их сценарий, чтобы разорвать привычный шаблон. Лучшее, что можно сделать в подобной ситуации – прекратить всякое общение с преступником.

Защита вашей безопасности и данных должна быть приоритетом. Рассказывайте своим друзьям и близким о возможных рисках и сценариях мошенничества, чтобы помочь им оставаться бдительными. Помните, знания о схемах мошенничества и методах защиты помогут вам избежать попадания в ловушку.

КРИБРУМ
Мы слушаем сеть

БЦ «Верейская плаза – 3»
ул. Верейская, 29, стр. 134
тел. +7 (499) 390-67-13
www.kribrum.ru