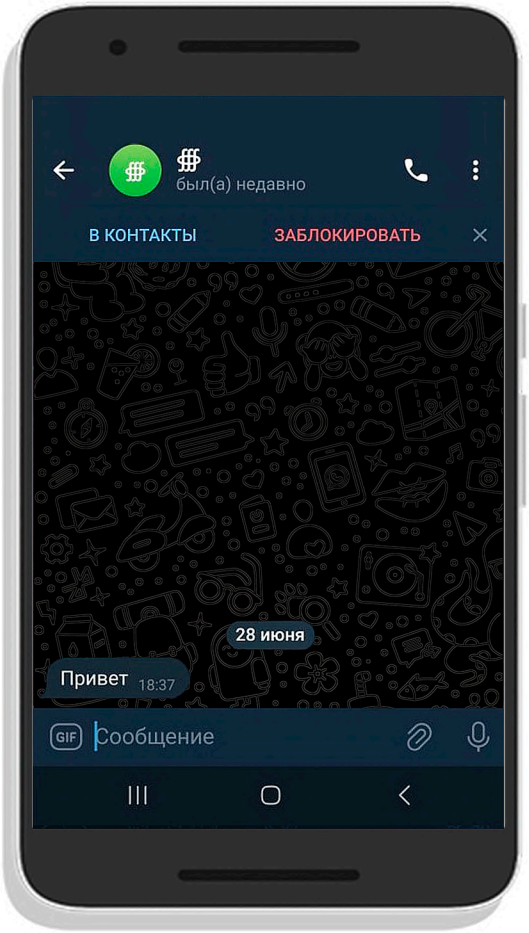
«БЕЗОПАСНАЯ РАБОТА В МЕССЕНДЖЕРАХ»

Личные данные
Не сообщайте свои личные данные незнакомцам в мессенджерах, данные для входа не передавайте никому.
Личной информацией может быть: ФИО, корпоративные и собственные телефонные номера, адреса электронной почты, должность, адреса проживания и работы и т.д.



Неизвестный отправитель
Сообщения от подозрительных, неизвестных отправителей стоит игнорировать, тем более, если в них содержатся ссылки и вложения. Отправителя добавьте в черный список.

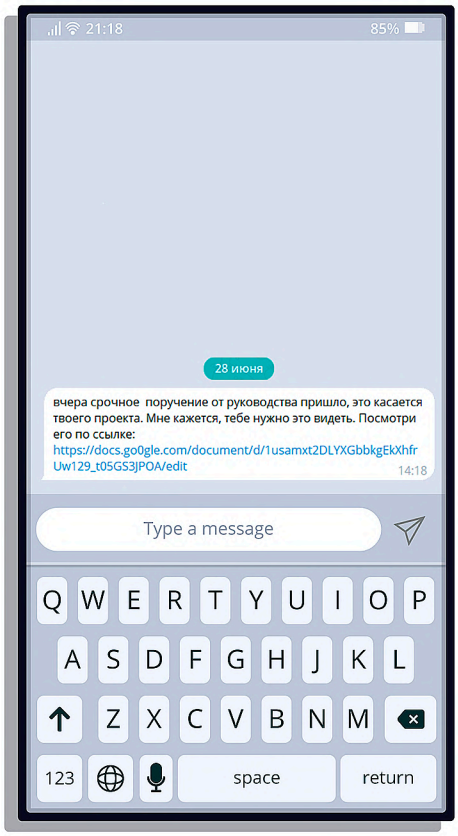
Вам могут написать «привет», ожидая вашего ответа. Ответив, вы добавите злоумышленника в «белый» список, и он получит возможность писать вам дальше. Такие сообщения лучше игнорировать. Если человеку будет нужно, он найдет другие способы связи.

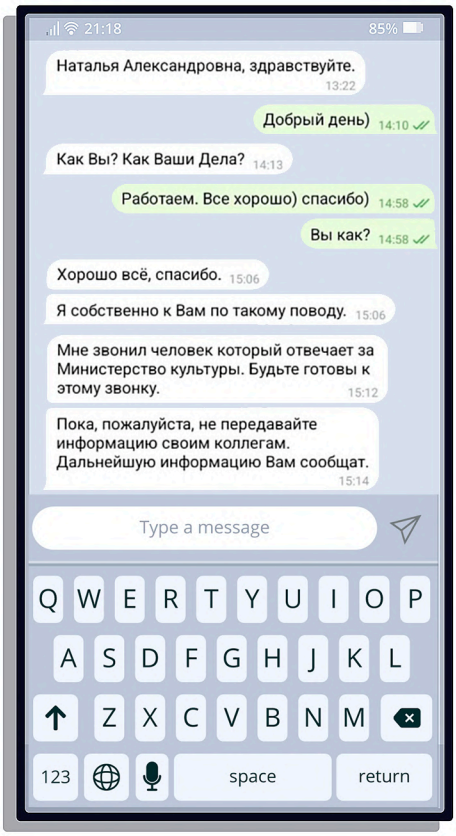
Сообщения от организаций
Помните, что банки, государственные ведомства, МВД и т.п. не будут решать с вами служебные вопросы по телефону и в мессенджерах.

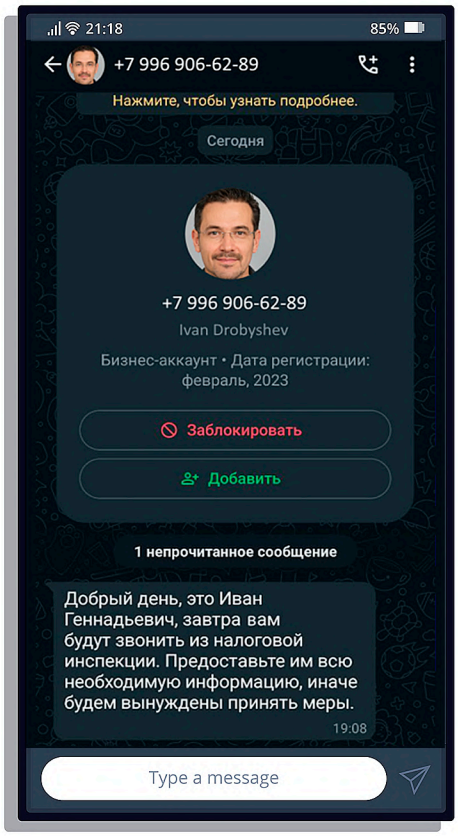
Доверяй, но проверяй

Если ваш знакомый или коллега отправляет вам подозрительное сообщение, свяжитесь с ним по другим, проверенным, каналам связи и уточните информацию.

Мошенники часто подделывают аккаунты и предупреждают о последующих звонках от государственных ведомств. Их цель — сделать вас более доверчивым к следующему звонку. Если вы получите предупреждение от «проверенного» источника о том, что вам, например, позвонит ФСБ, вы с большей вероятностью поделитесь конфиденциальной информацией.

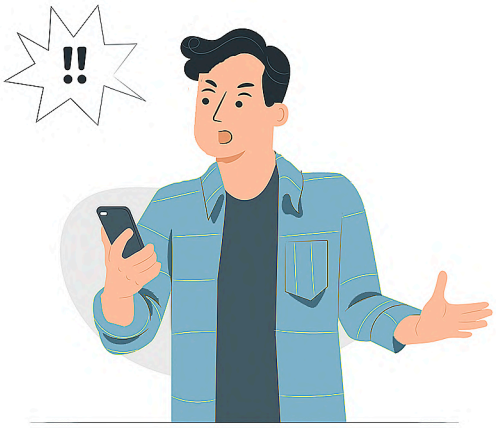


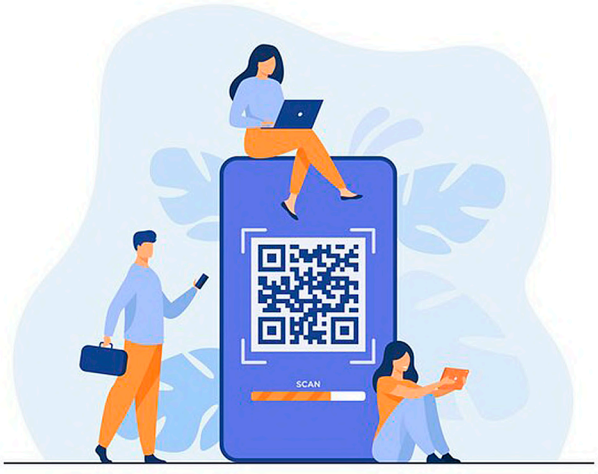




Эмоциональный отклик

Если текст сообщения слишком эмоционален, вы распознаете в нем манипуляции, в нем содержатся угрозы и давление, то задайте уточняющие вопросы. Возможно, это пишет злоумышленник.



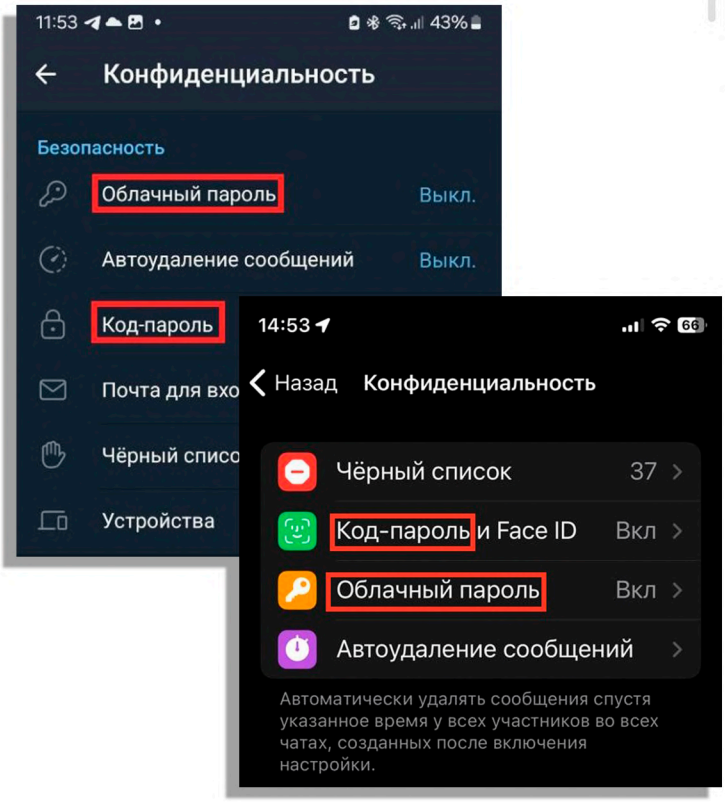


Ссылки, файлы и QR-коды

Если вам посылают ссылки, файлы и QR-коды в подозрительных сообщениях, связанных с работой, не спешите взаимодействовать с ними. Перешлите подозрительные сообщения в отдел информационной безопасности.

Голосовые и видеосообщения, звонки

При записи голосовых сообщений старайтесь не проговаривать рабочую и конфиденциальную информацию. В кадре видеосообщений не должны быть засвечены внутренние объекты предприятий.



Пароль

Установите код-пароль для доступа к вашему мессенджеру.

Это пригодится, если ваш телефон попадет к постороннему человеку. Так он не сможет прочитать ваши переписки.

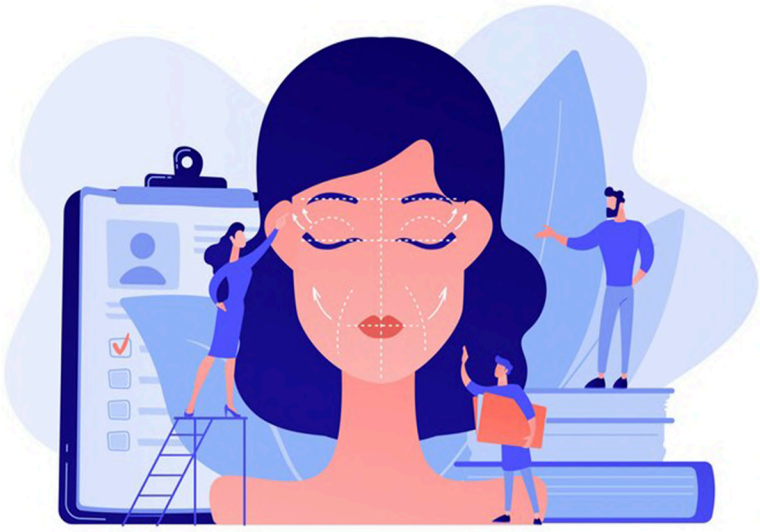
Также вы можете установить дополнительный облачный пароль, который будет запрашиваться при входе в аккаунт с нового устройства.

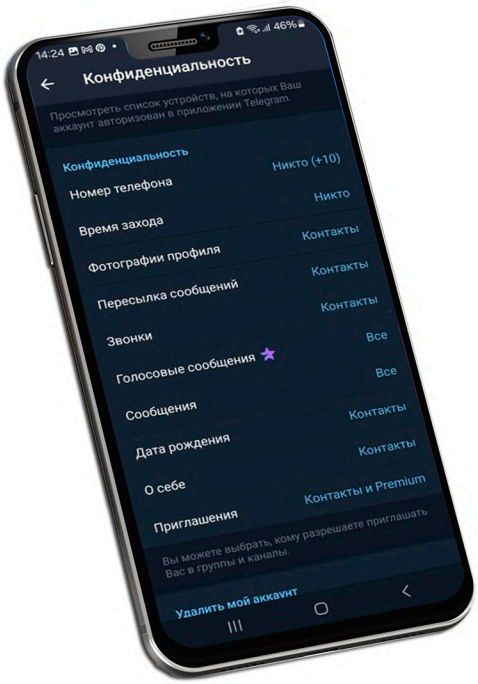
Поддельные аудио- и видеосообщения

Сегодня искусственный интеллект используется повсеместно, и злоумышленники могут с его помощью подделывать фото, аудио- и видеосообщения.

Обратите внимание на содержание таких сообщений: не кажется ли оно вам подозрительным? Может, в нем содержится необычная просьба? Также попробуйте проанализировать речь, голос, мимику и поведение человека по ту сторону экрана.

Попытайтесь вывести человека на телефонный разговор, поскольку программы пока с трудом генерируют голос в режиме реального времени.

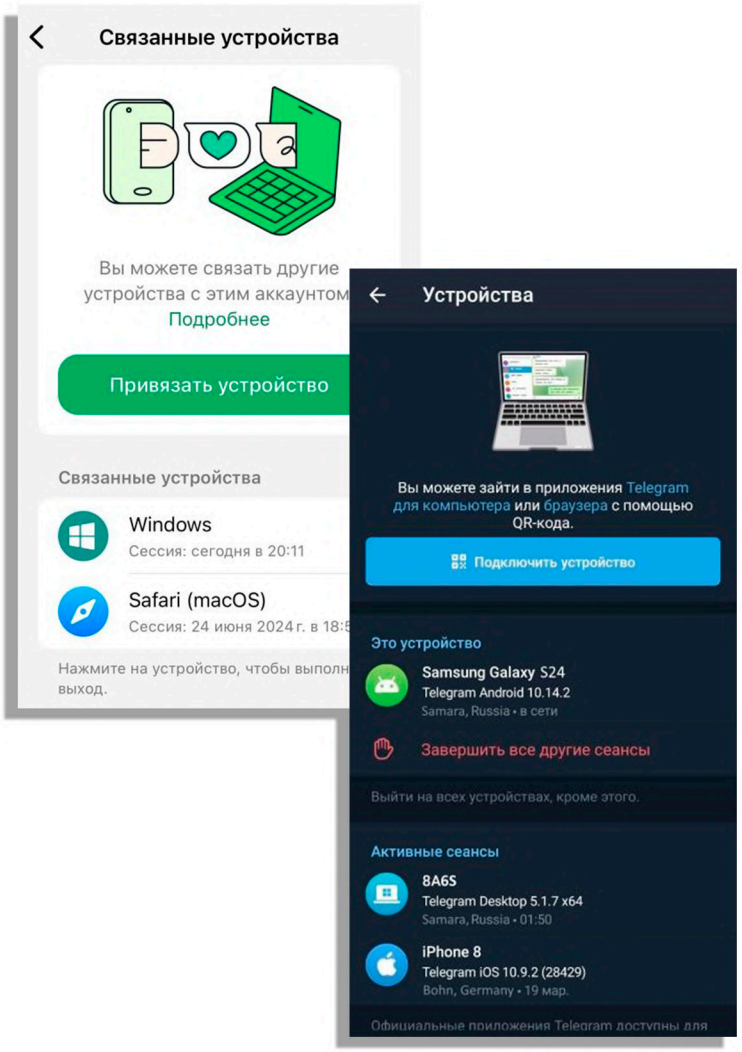




Настройки конфиденциальности
Задумайтесь, нужно ли незнакомцам видеть ваш номер телефона, если они могут написать вам сообщение? Зачем им знать, когда вы последний раз были в мессенджере?

Просмотрите и выберите в настройках конфиденциальности мессенджеров наиболее подходящие для вас параметры.

Проверка сеансов
В некоторых мессенджерах можно просмотреть актуальные сеансы, следует периодически их проверять.
Если вы увидели устройство, с которого вы не заходили в приложение, удалите лишнее устройство. Это мог быть злоумышленник, который взломал ваш аккаунт.



Обновление приложений
Регулярно обновляйте мессенджеры, которыми вы пользуетесь для работы. В обновлениях устраняются уязвимости безопасности.

С пожеланиями безопасности, StopPhish