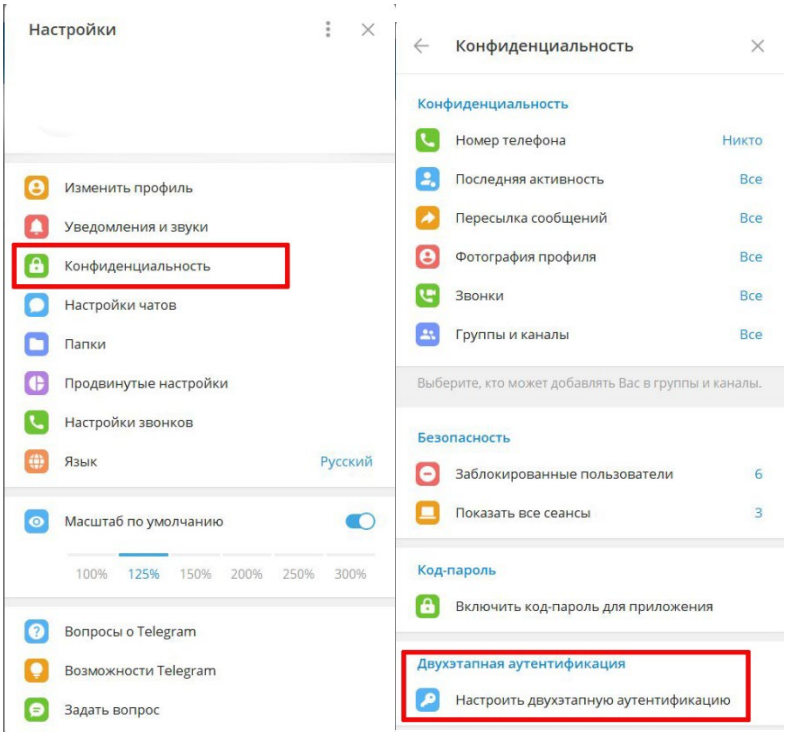
ПАМЯТКА ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ, СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ

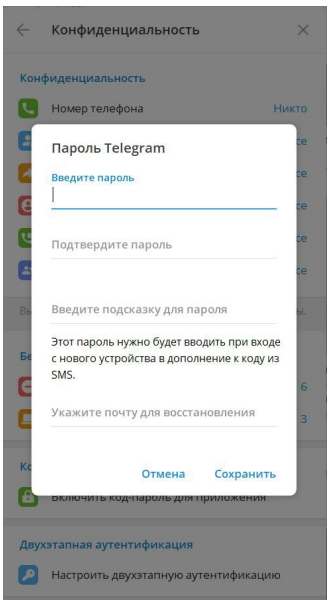
1. Настройте двухфакторную аутентификацию

Принцип прост: при входе в аккаунт вам нужно дважды подтвердить свою личность, введя сначала пароль, а затем код из SMS-сообщения, push-уведомления или сообщения от программы-генератора кодов. То есть хакерам для взлома страницы нужно не только узнать ваш пароль, но и получить дополнительный код.

Telegram

Войдите в настройки и откройте раздел «Конфиденциальность», там выберите пункт «Настроить двухэтапную аутентификацию» (на Android и в приложении для Windows) или «Облачный пароль» (на iOS).





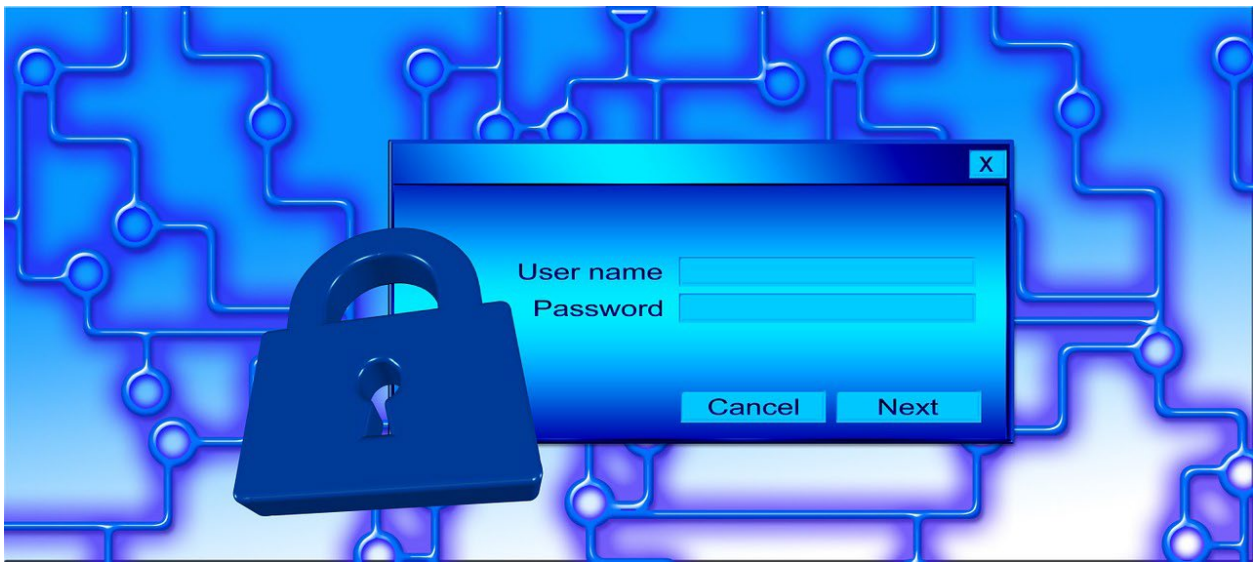
VIBER

Чтобы настроить PIN-код:

1. Откройте Viber на смартфоне
2. Нажмите на кнопку Ещё
3. Выберите Настройки
4. Выберите Конфиденциальность
5. Нажмите Двухэтапная проверка
6. Введите 6-значный PIN-код
7. Нажмите Далее
8. Введите PIN-код ещё раз
9. Нажмите Далее
10. На странице подтверждения вы увидите адрес email, который вы указали при регистрации учётной записи Viber.
    - Нажмите Далее, чтобы продолжить и завершить настройку двухэтапной проверки.
    - Если вы не указывали email ранее или хотите использовать другой email, введите желаемый адрес.
11. Вы получите письмо, с помощью которого вам нужно подтвердить свой адрес email, чтобы завершить настройку двухэтапной проверки.

2. Используйте надежные пароли

Прежде всего, постарайтесь создать разные пароли для каждой соцсети. Пароль должен быть достаточно длинным (минимум 10-12 знаков), содержать заглавные и строчные буквы, цифры, специальные символы. Чем более разнообразные знаки входят в пароль, тем труднее его подобрать.



Если вы используете для пароля слова или выражения, то переставьте в них порядок букв или слов, так вы усложните взломщикам подбор. Еще один способ – заменить отдельные буквы разными символами. Но учтите, что слишком очевидные замены вроде нуля вместо буквы «о» уже не работают и легко вычисляются хакерскими программами.

3. Закройте аккаунт от посторонних

Закройте в соцсетях информацию о вас и доступ к публикациям для посторонних, а также ограничьте круг тех, кто может переписываться с вами и добавлять в друзья. Это позволит избежать не только спама, но и рассылки вредоносных ссылок. Незнакомцы не смогут увидеть, например, список ваших друзей, чтобы разослать по нему сообщения с просьбой перевести денег.

В Telegram

- скройте свой номер в разделе «Конфиденциальность» – «Номер телефона»;
- запретите ссылку на вас при пересылке сообщений;
- запретите добавлять вас в группы;
- скройте свой сетевой статус, чтобы никто не знал, когда вы онлайн.

Дополнительно можно запретить звонки или скрыть фотографию профиля.

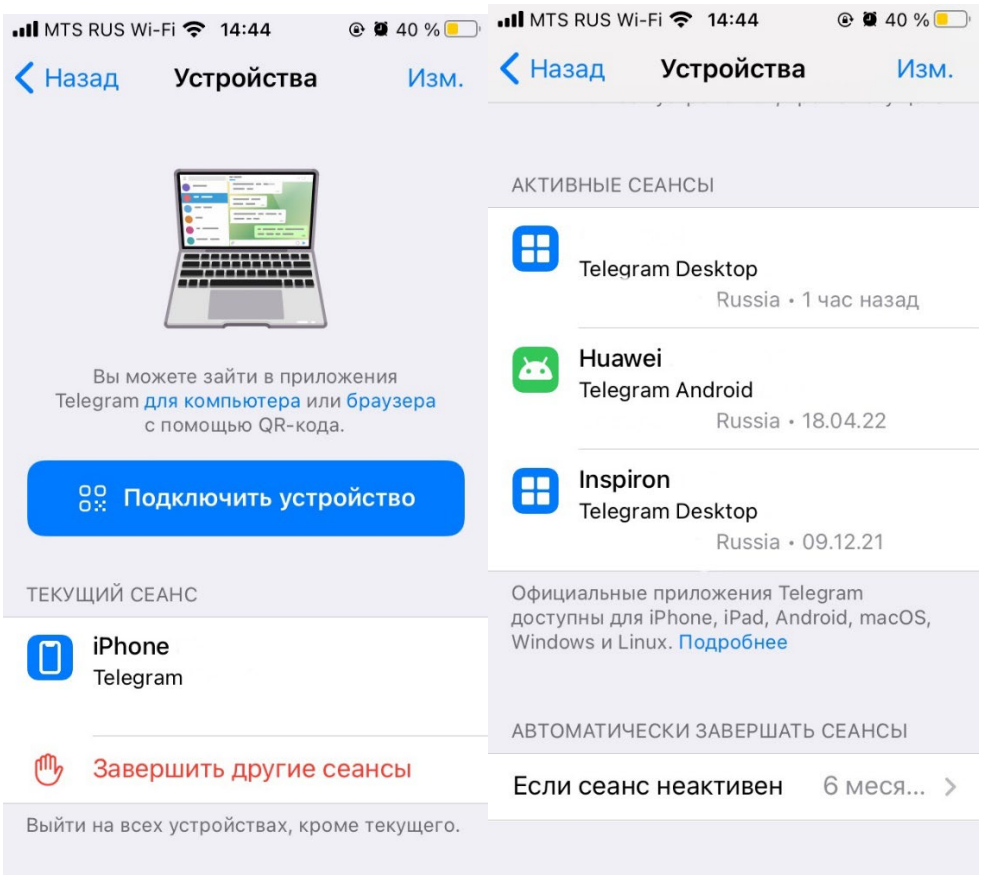
4. Завершайте сессии на устройствах, которыми не пользуетесь

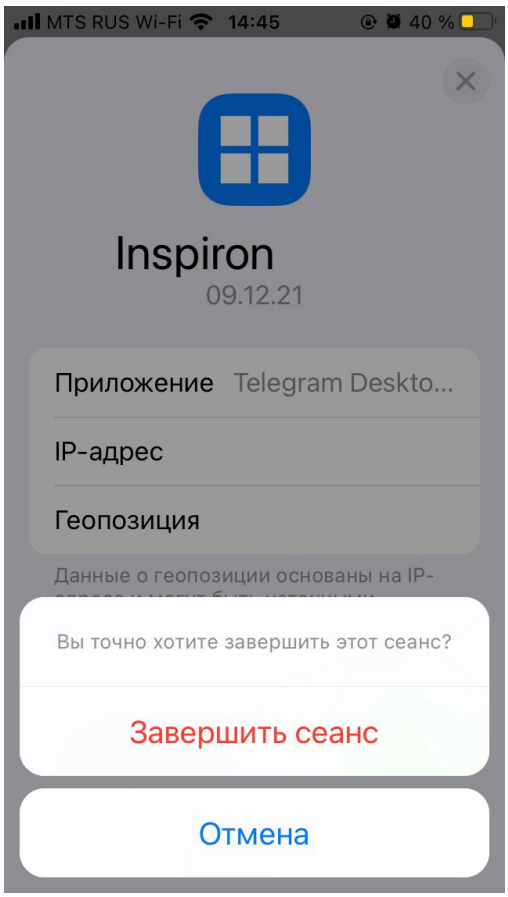
Зачастую мы пользуемся соцсетями на нескольких устройствах. Это удобно, однако создает пробел в безопасности. Гаджет с неоконченной сессией может попасть в руки мошенников, что облегчит им доступ к вашему аккаунту. Поэтому закрывайте сессии на устройствах, которыми не пользуетесь в данный момент – например, на планшете, рабочем ПК или запасном телефоне.

А если появилось подозрение, что вас взломали – посмотрите, с каких устройств и из каких локаций совершался вход в аккаунт. Если увидели подозрительные сессии, то нужно завершить их и срочно поменять пароль.

Telegram

В Telegram для закрытия сессий войдите в «Настройках» в раздел «Устройства». На экране отобразятся все сеансы: можно завершить все разом, кроме текущего.





5. Не используйте аккаунты в соцсетях для входа на сторонние сайты

Зачастую на разных сайтах предлагают авторизоваться с помощью аккаунта в социальных сетях или почте. Это очень соблазнительно: вместо долгой регистрации просто залогиниться через Telegram, Google или ВКонтакте.

Но так вы оставляете на сайте информацию для входа в ваш аккаунт. Даже если вы полностью доверяете ресурсу, никто не гарантирует, что он не будет взломан, а ваши данные не попадут в руки злоумышленников.

В наибольшей степени это касается онлайн-магазинов и любых сайтов, где вы проводите оплату банковскими картами. В этом случае угроза конфиденциальности возрастает, так как вы собираете платежные сведения и свои личные данные в одном месте.

6. Не доверяйте посторонним в интернете

Примите как данность: вы не знаете, кто скрывается за ником и фото в соцсети, даже если приходит сообщение от приятеля, с которым давно не общались.

Вот несколько правил, которые помогут при общении в социальных сетях:

- Не переписывайтесь с незнакомыми и малознакомыми людьми и не сообщайте им личную информацию.

- Не открывайте ссылки, видео, фото и любые документы, если вы не уверены в адресате. Когда знакомый, с которым вы не переписывались годами, присылает видео с котиками – это повод насторожиться, а не открывать его.
- Не участвуйте в сомнительных розыгрышах и акциях. Если не повезет – откроете вредоносную ссылку или передадите сведения о себе мошенникам.
- Если в беседе со знакомым вас что-то насторожило, например, странное обращение, стиль письма, ошибки, неожиданный вопрос, просьба перевести деньги и т.п., то задайте ему личный вопрос. Это поможет понять, взломан ли аккаунт.

7. Не реагируйте на шантаж

Увы, но сетевой шантаж — не такая уж редкость. Злоумышленники взламывают аккаунт и находят компрометирующий контент либо вообще создают его самостоятельно с помощью монтажа, а потом требуют деньги, угрожая распространить приватные фото или видео по вашим знакомым. Если кратко: не паникуйте и не идите на поводу у преступников. Лучше всего не вступать с шантажистом в диалог и тем более нельзя переводить ему деньги.