Краевое государственное автономное образовательное учреждение
дополнительного образования «Центр развития творчества детей
(Региональный модельный центр дополнительного образования детей Хабаровского края)»

ПАМЯТКА

ДВУХЭТАПНАЯ АУТЕНТИФИКАЦИЯ АККАУНТОВ В СОЦИАЛЬНЫХ СЕТЯХ

г. Хабаровск, 2021 год

Памятка «Двухэтапная аутентификация аккаунтов в социальных сетях» / Сост. Е.А. Фомина – г. Хабаровск: КГАОУ ДО РМЦ, 2021. – 4 с.

Ответственный за выпуск: О.В. Монахова

ДВУХЭТАПНАЯ АУТЕНТИФИКАЦИЯ АККАУНТОВ В СОЦИАЛЬНЫХ СЕТЯХ

Практически любая ваша учетная запись в Интернете может быть взломана. После многочисленных широко распространенных нарушений за последние несколько лет технологические компании работали вместе над разработкой стандарта, который оставил бы пароли в прошлом, заменив их более безопасными методами, такими как биометрические или PIN-коды для входа в систему, которые не требуют передачи данных в интернет.

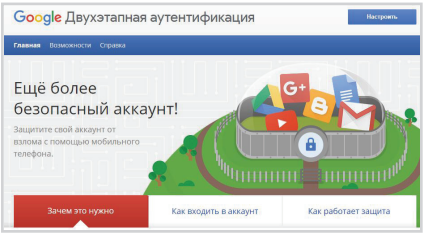
Но пока эти стандарты все еще принимаются, следующий лучший способ защитить ваши учетные записи - это двухфакторная аутентификация или 2FA. Это процесс, который предоставляет веб-службам вторичный доступ к владельцу учетной записи (вам) для проверки попытки входа в систему. Обычно это включает номер телефона или адрес электронной почты. Вот как это работает: когда вы входите в службу, вы используете свой мобильный телефон, чтобы подтвердить свою личность, щелкнув ссылку в текстовом или электронном письме, или введя номер, отправленный приложением для проверки подлинности.

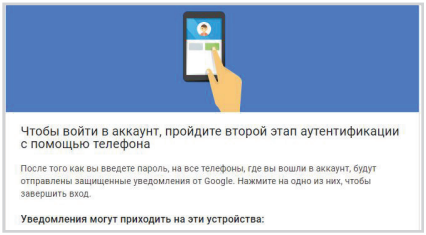
Если вам нужно что-то, что не зависит от программного обеспечения для обеспечения безопасности вашего устройства, вы также можете выбрать электронный ключ. Оборудование на основе USB или NFC подключается к вашему компьютеру или мобильному устройству для аутентификации, что затрудняет перехват хакерам, поскольку ключи безопасности не могут быть дублированы. Для получения дополнительной информации о том, как работают электронные ключи, ознакомьтесь с нашим руководством по электронным ключам.

GOOGLE

Самый простой способ включить двухфакторную аутентификацию в своих учетных записях Google (например, Gmail, YouTube или Google Maps) - это перейти на главную целевую страницу двухфакторной аутентификации и нажать «Начать».

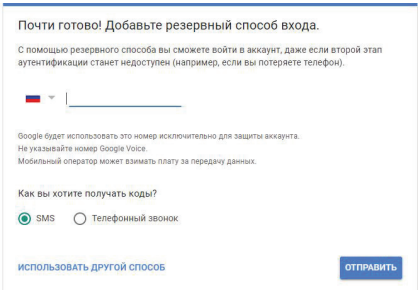
Вам будет предложено войти в систему, а затем выбрать свое мобильное устройство из списка. Если Google удастся отправить сообщение на этот телефон, вам будет предложено ввести номер телефона, а затем вы сможете вы-





брать, хотите ли вы получать коды подтверждения. текстовым сообщением или телефонным звонком. Опять же, Google опробует выбранный вами метод.

После этого Google сначала отправит на ваш телефон запросы, которые позволят вам просто выбрать «Да» или «Нет» при попытке входа в систему. Если это не сработает, он отправит текстовое сообщение или телефонный звонок.



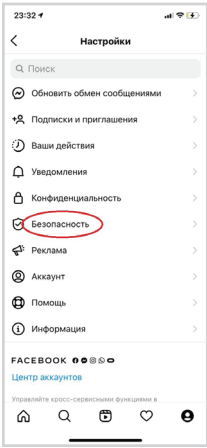
После включения 2FA Google отправит уведомление с просьбой пройти аутентификацию.

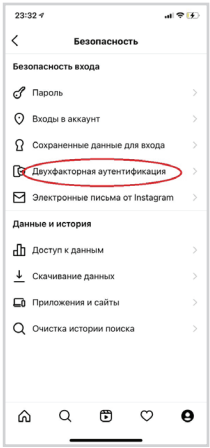
Вы также можете сгенерировать резервные коды для автономного доступа. Google генерирует 10 кодов за раз, и они предназначены для одноразового использования, поэтому после того, как вы успешно применили один, вычеркните его (при условии, что вы их распечатали), так как он больше не будет работать.

INSTAGRAM

Instagram добавил двухфакторную аутентификацию в свое мобильное приложение в 2017 году, но теперь вы также можете активировать его через Интернет.

Чтобы активировать двухфакторную аутентификацию в своем мобильном приложении, нажмите на свой профиль и выберите гамбургер-меню в правом верхнем углу. Найдите «Настройки»> «Безопасность», где вы найдете пункт меню «Двухфакторная аутентификация».

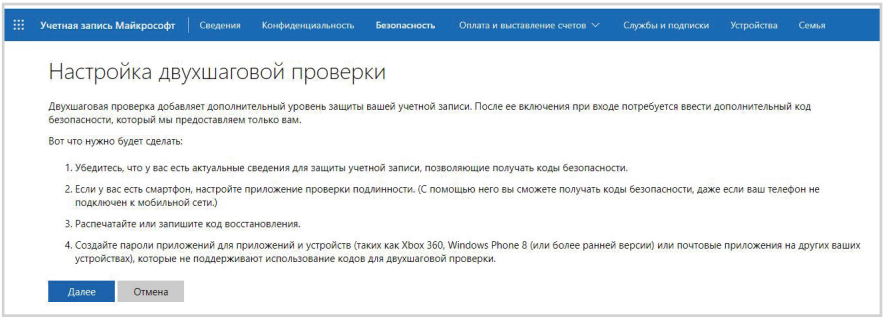




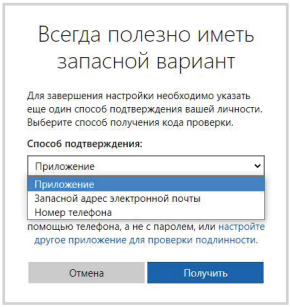
Здесь вы можете выбрать между проверкой на основе текстового сообщения или кодом, отправленным в ваше приложение для проверки подлинности.

MICROSOFT

Войдите в свою учетную запись Microsoft и найдите меню «Настройки безопасности». Найдите раздел «Двухэтапная проверка» и щелкните ссылку настройки.



Вы пройдете через шаги, необходимые для использования приложения Microsoft Authenticator или другого приложения для проверки подлинности.

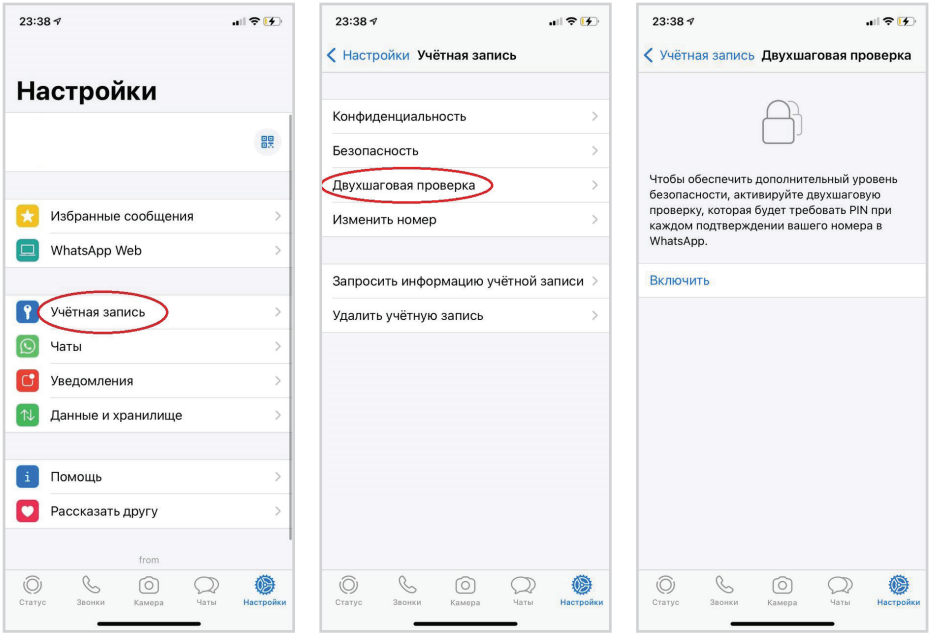


Вы также сможете создавать пароли для приложений, которые не принимают двухфакторную аутентификацию.

WHATSAPP

Откройте WhatsApp и найдите меню «Настройки» под значком с точками в правом верхнем углу. Найдите в разделе «Учетная запись»> «Двухэтапная проверка»> «Включить».

Приложение попросит вас ввести шестизначный PIN-код для проверки. При желании вы можете добавить адрес электронной почты на случай, если забудете свой PIN-код.



Наличие электронной почты, связанной с вашей учетной записью WhatsApp, важно, поскольку служба не позволит вам перепроверить себя, если вы использовали WhatsApp в течение последних семи дней и забыли свой PIN-код. Поэтому, если вы не можете ждать неделю, чтобы повторить проверку, полезно ввести адрес электронной почты, чтобы вы могли войти в систему или отключить 2FA. В том же ключе: будьте осторожны с электронными письмами, призывающими вас отключить двухфакторную аутентификацию, если вы сами этого не запрашивали.

Памятка «Двухэтапная аутентификация аккаунтов в социальных сетях»

Краевое государственное автономное образовательное учреждение
дополнительного образования «Центр развития творчества детей
(Региональный модельный центр дополнительного образования детей
Хабаровского края)»
680000, г. Хабаровск, ул. Комсомольская, 87
тел. / факс: (4212) 30-57-13
Инстаграм: @dop.obrazovanie27
e-mail: yung_khb@mail.ru
http://www.kcdod.khb.ru
Подписано в печать: 30.09.2021 г.