

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-

The screenshot shows the Google Two-step Verification landing page. It features a central illustration of a smartphone displaying various Google services like Google+, YouTube, and Gmail, all protected by a lock. The text "Ещё более безопасный аккаунт!" (Even more secure account!) is prominently displayed. Below the illustration are three buttons: "Зачем это нужно" (Why do I need it?), "Как войти в аккаунт" (How to log in to your account), and "Как работает защита" (How protection works). At the top right, there's a "Настройки" (Settings) button.

This screenshot shows the second step of setting up Google Two-step Verification. It features a large image of a hand holding a smartphone with a lock icon on its screen. The text "Чтобы войти в аккаунт, пройдите второй этап аутентификации с помощью телефона" (To log in to your account, complete the second step of verification using your phone) is at the top. Below it, a note says "После того как вы введете пароль, на все телефоны, где вы вошли в аккаунт, будут отправлены защищенные уведомления от Google. Нажмите на одно из них, чтобы завершить вход." (After you enter your password, secure notifications from Google will be sent to all phones where you've logged in. Tap one of them to finish logging in.) At the bottom, it says "Уведомления могут приходить на эти устройства:" (Notifications may come to these devices: [list of device icons]).

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.

This screenshot shows the Instagram settings menu. On the left, under "Настройки" (Settings), the "Безопасность" (Security) option is selected. On the right, under "Безопасность" (Security), the "Двухфакторная аутентификация" (Two-factor authentication) option is highlighted with a red oval. Other options listed include "Пароль" (Password), "Входы в аккаунт" (Logins), "Сохраненные данные для входа" (Saved login data), "Электронные письма от Instagram" (Email from Instagram), "Данные и история" (Data and history), "Доступ к данным" (Data access), "Скачивание данных" (Download data), "Приложения и сайты" (Apps and sites), and "Очистка истории поиска" (Clear search history).

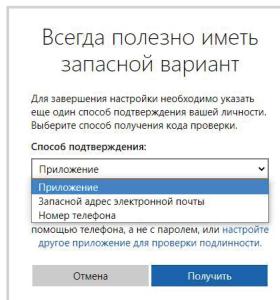
This screenshot shows the Instagram settings menu. On the left, under "Настройки" (Settings), the "Безопасность" (Security) option is selected. On the right, under "Безопасность" (Security), the "Двухфакторная аутентификация" (Two-factor authentication) option is highlighted with a red oval. Other options listed include "Пароль" (Password), "Входы в аккаунт" (Logins), "Сохраненные данные для входа" (Saved login data), "Электронные письма от Instagram" (Email from Instagram), "Данные и история" (Data and history), "Доступ к данным" (Data access), "Скачивание данных" (Download data), "Приложения и сайты" (Apps and sites), and "Очистка истории поиска" (Clear search history).

MICROSOFT

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

The screenshot shows a Microsoft account settings page. At the top, there's a navigation bar with links like 'Учетная запись Microsoft', 'Сведения', 'Конфиденциальность', 'Безопасность' (Security), 'Оплата и выставление счетов' (Billing), 'Службы и подписки' (Services and Subscriptions), 'Устройства' (Devices), and 'Семья' (Family). The main content area has a title 'Настройка двухшаговой проверки' (Configure two-step verification). Below it, a note says: 'Двухшаговая проверка добавляет дополнительный уровень защиты вашей учетной записи. После ее включения при входе потребуется ввести дополнительный код безопасности, который мы предоставляем только вам.' (Two-step verification adds an extra layer of security to your account. After enabling, you will need to enter an additional security code that we provide to you only.) A section titled 'Вот что нужно будет сделать:' (What you'll need to do) lists four steps: 1. Убедитесь, что у вас есть актуальные сведения для защиты учетной записи, позволяющие получать коды безопасности. (Make sure you have up-to-date information for protecting your account, such as a mobile phone number or email address.) 2. Если у вас есть смартфон, настройте приложение проверки подлинности. (If you have a smartphone, set up the Authenticator app.) 3. Распечатайте или запишите код восстановления. (Print or write down the recovery code.) 4. Создайте пароли приложений для приложений и устройств (таких как Xbox 360, Windows Phone 8 (или более ранней версии) или почтовые приложения на других устройствах), которые не поддерживают использование кодов для двухшаговой проверки. (Create app passwords for apps and devices that don't support two-step verification codes.) At the bottom are 'Далее' (Next) and 'Отмена' (Cancel) buttons.

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

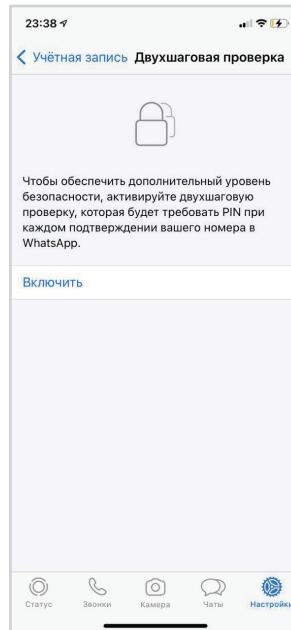
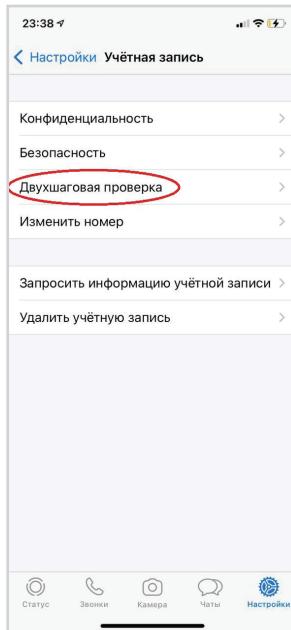
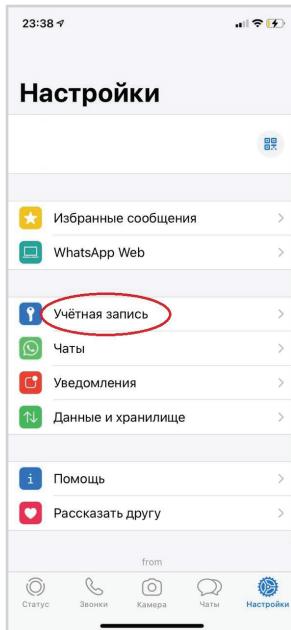


Вы также сможете создавать пароли для приложений, которые не принимают двухфакторную аутентификацию.

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.