



**Действуйте сейчас.
Оставайтесь
в безопасности.**

actnowstaysecure.gov.au

Чем вы рискуете в Интернете?

Поскольку технологии стремительно развиваются, и мы проводим все больше времени в Интернете, австралийцы остаются уязвимыми для кибератак.

Кампания «Действуйте сейчас. Оставайтесь в безопасности» обучает австралийцев простым действиям по кибербезопасности, которые каждый может предпринять, чтобы защитить себя в Интернете.

Действуйте сейчас. Оставайтесь в безопасности.

Как обеспечить безопасность в сети

Используйте уникальную и надежную парольную фразу для каждого аккаунта

Использование уникальной и надежной парольной фразы для каждого из ваших онлайн-аккаунтов — одно из самых эффективных действий, которые вы можете предпринять, чтобы оставаться в безопасности в сети.

Парольная фраза — это более надежный пароль. Она содержит последовательность случайных слов. Их легче запомнить, но сложнее угадать киберпреступникам.

Чтобы обеспечить надежность и уникальность, убедитесь, что ваши парольные фразы:

- ✓ состоят из четырех или более случайных слов
- ✓ содержат 15 или более знаков
- ✓ различны для каждого аккаунта
- ✓ не содержат идентифицирующую информацию, такую как имена, фамилии, даты рождения или адреса
- ✓ включают символы, заглавные буквы или цифры, если это требуется веб-сайтом или службой.

Рассмотрите возможность использования менеджера паролей для создания и хранения уникальных паролей.

Установите все обновления программного обеспечения, чтобы обеспечивать безопасность ваших устройств

Постоянная установка обновлений программного обеспечения для всех ваших подключенных к Интернету устройств (например, телефона, ноутбука или смарт-часов) имеет решающее значение для обеспечения вашей безопасности в Интернете.

Обновления программного обеспечения устраняют слабые места или пробелы в системе безопасности ваших устройств. Установка регулярных обновлений обеспечит безопасность ваших устройств и усложнит доступ к ним киберпреступников.

Включите автоматические обновления и обязательно устанавливайте их при появлении соответствующего запроса.

Всегда настраивайте многофакторную аутентификацию

Включайте многофакторную аутентификацию, где это возможно, чтобы добавить дополнительный уровень безопасности для всех ваших аккаунтов в Интернете.

Многофакторная аутентификация требует двух или более методов проверки для входа в ваш аккаунт. Например, после ввода пароля или парольной фразы вам будет предложено предоставить вторую проверку, такую как ввод кода, отправленного вам через приложение-аутентификатор, электронную почту или текстовое сообщение.

Многофакторная аутентификация защищает ваш аккаунт, даже если один из ваших других методов аутентификации (например, парольная фраза) скомпрометирован.



**Действуйте сейчас.
Оставайтесь
в безопасности.**

actnowstaysecure.gov.au

Хотите больше способов обеспечения безопасности в Интернете?

Ищете больше способов обеспечения кибербезопасности? Вот несколько других действий, которые вы можете предпринять, чтобы защитить себя в Интернете.

Будьте осторожны при использовании общественного Wi-Fi

При использовании общественного Wi-Fi не получайте доступ к какой-либо конфиденциальной или личной информации, поскольку соединение не защищено. Это касается ваших социальных сетей, электронной почты или онлайн-банкинга. Любая введенная вами информация может стать доступной киберпреступникам.

Регулярно проверяйте и обновляйте настройки конфиденциальности и местоположения

Важно регулярно проверять настройки конфиденциальности и местоположения, чтобы убедиться, что вы случайно не делитесь личной или идентифицирующей информацией о себе с другими людьми.

Настройки для проверки включают настройки конфиденциальности в ваших аккаунтах в социальных сетях и отслеживание геолокации в ваших приложениях и устройствах.

Поговорите с друзьями и семьей о том, как обеспечивать кибербезопасность

Образование и осведомленность имеют решающее значение для обеспечения вашей безопасности, безопасности вашей семьи и друзей в Интернете, особенно если вы используете общие устройства, подключенные к Интернету. Обсуждение этого вопроса с вашей сетью позволяет вам помнить о кибербезопасности и гарантирует, что члены сети получают самую свежую информацию о том, как защитить себя в Интернете.

Узнайте, как распознавать мошенничество

Мошенники обманывают людей, заставляя их платить деньги или предоставлять свою личную информацию.

Никогда не давайте деньги или личную информацию кому-либо, если вы не уверены, с кем имеете дело. Проверьте, связавшись с человеком или организацией, используя данные, которые вы нашли на официальном сайте или в приложении.

Сообщайте о кибератаках и инцидентах

Сообщение о мошенничестве или киберинцидентах имеет решающее значение для помощи правительству в выявлении новых тенденций, оповещения общества и помощи вам в восстановлении после киберинцидента.

Изучите простые шаги по защите себя на сайте actnowstaysecure.gov.au



**Действуйте сейчас.
Оставайтесь
в безопасности.**

actnowstaysecure.gov.au