



Australian Government



Действуйте сейчас.
Оставайтесь в безопасности.

Как обезопасить себя в интернете

Легкочитаемая версия



Как пользоваться этим руководством



Мы Правительство Австралии.

Мы написали это руководство.



Некоторые слова выделены **жирным шрифтом**.

Их значение мы объясняем отдельно.

Полный список этих слов есть на странице 28.



Можно попросить того, кому доверяете, помочь:

- изучить это руководство
- найти дополнительную информацию.



Это легкочитаемое изложение другого руководства.

В него вошло только самое главное.



Другое руководство есть на нашем сайте.

www.actnowstaysecure.gov.au

Что в этом руководстве?

Об этом руководстве	4
---------------------	---

Защитите свои аккаунты	6
------------------------	---

Проверьте настройки защиты данных	10
-----------------------------------	----

Защитите свои устройства	16
--------------------------	----

Мошенничество	20
---------------	----

Не молчите	25
------------	----

Список слов	28
-------------	----

Обращайтесь к нам	30
-------------------	----

Об этом руководстве



Нам всем приходится задумываться о безопасности в сети.

Это называется **кибер**безопасность.



«Кибер-» значит «относится к интернету».



Это руководство о том, как защитить себя в интернете.

Например, от **киберпреступности**.

Киберпреступность – это преступность в интернете.



Например, через интернет преступники могут:

- похитить ваши персональные данные
- завладеть вашими аккаунтами или профилями.

Киберпреступности подвержены все устройства.



В том числе:

- компьютер
- смартфон
- смарт-часы.



От киберпреступности есть меры защиты.



О них мы расскажем на следующих страницах.

Защитите свои аккаунты



Стоит подумать о том, как защитить свои аккаунты.

Выбирайте сложные и разные кодовые фразы



Кодовая фраза – это, по сути, усиленный пароль.

Злоумышленнику очень трудно ее подобрать.



Сложные и разные кодовые фразы – одна из лучших защит для учетных записей.



На каждый аккаунт должна быть своя кодовая фраза.



В сильных кодовых фразах:

- не менее 4 случайных слов
- не менее 15 букв и цифр.



Можно некоторые буквы сделать заглавными.



Можно использовать такие символы, как:

- тире
- знак доллара
- символ @ («собака»).



Не стоит включать в кодовую фразу персональные данные.



Например:

- дату своего рождения
- имена членов семьи или домашних животных.

Добавьте дополнительные шаги для входа в аккаунты



Защитить аккаунты поможет **многофакторная аутентификация (MFA)**.

MFA – это когда при входе в аккаунт каждый раз выполняется несколько разных проверок.



Например, сначала запрашивается кодовая фраза.

Затем нужно ввести код, который пришел на телефон.

Получить код можно разными способами:



- через приложение-генератор кода на телефоне



- по электронной почте



- по СМС.



MFA усложняет злоумышленнику вход в ваш аккаунт.

Даже если он знает кодовую фразу.

Проверьте настройки защиты данных



Можно проверить, настроена ли у вас защита данных в интернете.



Речь идет о настройках:

- в аккаунтах
- на устройствах
- в приложениях.



Вы можете:

- поменять настройки
- разрешить или запретить приложениям читать ваши данные.

Чтобы найти на устройстве меню настроек, можно:



- поискать значок «шестеренка»
- или
- ввести в поиск «settings» или «настройки».



Настройки приложения или аккаунта можно найти в меню.

Кнопка меню часто обозначается тремя горизонтальными черточками.



Некоторые настройки открывают доступ к данным о том:

- кто вы
- где находитесь
- где живете.



Выкладывать эти сведения в интернет
опасно: можно стать жертвой
киберпреступников.



Завладев вашими данными,
киберпреступники могут выдавать себя за
вас.

Для этого могут использоваться такие сведения, как:



- ваш домашний адрес



- имена членов вашей семьи



- имена ваших домашних животных.



Профили в соцсетях можно настроить так, чтобы их видели только ваши знакомые.

Например, это можно сделать на Фейсбуке.



Это так называемые настройки конфиденциальности (privacy settings).



Можно также управлять **определением местоположения**.

Эта функция показывает, где находится устройство.



Определение местоположения можно включать и отключать.

Можно выбрать, какие приложения будут знать, где вы находитесь.



Это можно сделать:

- в аккаунтах
- на устройствах
- в приложениях.

Некоторые приложения могут запрашивать разрешение:



- пользоваться камерой



- просматривать ваши фотографии.



Давать доступ к камере и фотографиям можно только знакомым приложениям.

Защитите свои устройства



Стоит подумать о том, как защитить свои устройства, чтобы не рисковать в интернете.

Например, телефон или смарт-часы.



Это важно для устройств, которые выходят в интернет.

Устанавливайте обновления



Устройства можно обновлять, чтобы защитить их от угроз в интернете.

Например, обновляются телефоны и ноутбуки.



На самом устройстве это может называться «обновление ПО» (software update).



Обновления помогают устройству защититься от киберугроз.



Можно настроить на устройстве автоматическое обновление.



Подробнее о том, как обновлять устройства, можно узнать на нашем сайте.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Публичные сети Wi-Fi



Будьте осторожны в **публичных сетях Wi-Fi**.



Публичная сеть Wi-Fi – это бесплатный беспроводной интернет в общественных местах.



Например, в:

- кафе
- аэропорту
- гостинице.



Выходя в интернет через публичный Wi-Fi, не вводите на сайтах конфиденциальную информацию.



Например:

- банковские реквизиты
- пароли от электронной почты
- пароли от соцсетей.



Через публичный Wi-Fi злоумышленники иногда могут:

- видеть, чем вы занимаетесь в интернете
- считывать вашу информацию.

Это связано с тем, что:



- публичными сетями Wi-Fi может пользоваться кто угодно



- в них сложнее защитить устройства.



Подробнее о том, как защитить себя в публичных сетях Wi-Fi, вы узнаете на нашем сайте.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Мошенничество



Мошенничество – это ситуация, когда:

- вас пытаются обмануть
- у вас пытаются забрать деньги.



Мошенник – это тот, кто занимается мошенничеством.

Мошенники могут пытаться вас обмануть:



- СМС-сообщением или звонком
- электронным письмом
- в социальных сетях
- на сайтах в интернете.



Они могут вести себя дружелюбно.

Но при этом обманом выуживать у вас данные.

Заполучив данные, они могут:



- проникать в ваши аккаунты



- выдавать себя за вас



- красть у вас деньги.

Мошенники могут в том числе:



- создавать фальшивые аккаунты, чтобы вас обмануть



- присылать ссылки и рекламу, чтобы вы на них нажали.

Как распознать мошенничество

Признаки мошенничества:



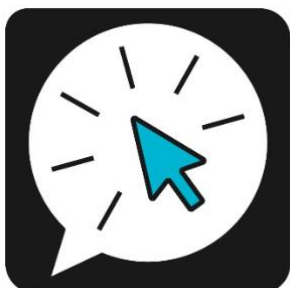
- вас просят срочно что-то сделать



- вам предлагают много денег



- у вас просят деньги



- вас просят перейти по ссылке.



Мошенники могут притворяться солидной организацией.

Например, вашим банком.



Это делается для того, чтобы выманить у вас персональные данные.



Если есть подозрение, что собеседник мошенник, прекратите общение.



Проверьте, тот ли он, за кого себя выдает.

Можно связаться с человеком или организацией по контактным данным, которым вы доверяете и которые нашли сами.



Если ситуация подозрительная, срочно примите меры защиты.

Как сообщить о мошенничестве



Scamwatch помогает жителям Австралии:

- знать уловки мошенников
- сообщать о фактах мошенничества.



Помогает Scamwatch и тем жителям Австралии, кто столкнулся с мошенничеством.



Сообщить о факте мошенничества можно на сайте Scamwatch.

www.scamwatch.gov.au/report-a-scam

Не молчите



Не стесняйтесь говорить о безопасности в интернете.

В частности:



- сообщайте о киберпреступлениях



- делитесь знаниями с семьей и друзьями.



О том, где и как высказываться, мы расскажем на следующих страницах.

Сообщайте о киберпреступлениях

Сообщения о киберпреступлениях помогают государству:



- разоблачать киберпреступников



- защищать население.



Сообщайте о киберпреступлениях на сайте ReportCyber.

www.cyber.gov.au/report

Говорите о кибербезопасности с родными и друзьями



Имеет смысл делиться советами по кибербезопасности с родными и друзьями.

Может быть, у них тоже есть чему поучиться.



Ваши знания о безопасности в интернете помогут защитить вас самих и окружающих.



Особенно это важно, если у вас одно устройство на несколько человек.

Список слов

В этом списке объяснено значение слов, набранных в этом руководстве **жирным** шрифтом.



Кибер-

«Кибер-» значит «относится к интернету».

Киберпреступность

Киберпреступность – это преступность в интернете.



Например, через интернет преступники могут:

- похитить ваши персональные данные
- завладеть вашими аккаунтами.



Определение местоположения

Эта функция показывает, где находится устройство.



Многофакторная аутентификация (MFA)

MFA – это когда при входе в аккаунт каждый раз выполняется несколько разных проверок.



Кодовая фраза

Кодовая фраза – это, по сути, усиленный пароль.

Злоумышленнику очень трудно ее подобрать.



Публичная сеть Wi-Fi

Публичная сеть Wi-Fi – это бесплатный беспроводной интернет в общественных местах.



Мошенничество

Мошенничество – это ситуация, когда:

- вас пытаются обмануть
- у вас пытаются забрать деньги.



Мошенники

Мошенник – это тот, кто занимается мошенничеством.

Обращайтесь к нам



Звоните на горячую линию по кибербезопасности (Australian Cyber Security Hotline).

1300 292 371



Заходите к нам на сайт.

www.actnowstaysecure.gov.au



Сообщайте о киберпреступлениях на сайте ReportCyber.

www.cyber.gov.au/report



Этот легкочитаемый документ подготовлен Information Access Group с использованием стоковых фотографий и пользовательских изображений. Запрещается заимствовать изображения без разрешения. Все вопросы об изображениях можно задать на сайте www.informationaccessgroup.com. Номер заказа 6342.
