

# **“Вас хотят взломать и скомпрометировать”: что вы знаете о безопасности в интернете?**

Пройдите тест CABAR.asia и узнайте, хорошо ли вы знаете, как защитить себя в интернете и что делать, если вас взломали?

Во время пандемии коронавируса практически все ушло в онлайн, а многие компании перешли на удаленный способ работы. Вместе с этим выросло количество случаев мошенничества в интернете, спекуляции на теме Covid-19 и взломов аккаунтов пользователей соцсетей.

10 июля активист из Кыргызстана Урмат Джаныбаев сообщил, что его аккаунт в Facebook был взломан. Кроме него о таких же случаях и попытках взлома сообщали другие кыргызстанцы. В том числе журналисты и активисты.

Помимо изменения или удаления аккаунта хакеры могут получить доступ к рабочей информации, личным фотографиям, видео, а также перепискам. Все это они могут использовать для шантажа или давления на пользователей.

17 июля техподдержка Twitter сообщила о взломе 130 аккаунтов, среди которых были знаменитости, бизнесмены, политики. Предлагаем почувствовать себя на месте последних и пройти тест и узнать, что вы знаете про сетевую безопасность.

Однако нужно помнить, что взламывают не только известных и публичных людей. Жертвой мошенников может стать любой пользователь. Хорошо ли вы знаете, как защитить себя в интернете и что делать если вас взломали?

**“Вас хотят  
взломать и  
скомпрометирова  
ть”: что вы  
знаете о  
безопасности в  
интернете?**

Пройдите тест [CABAR.asia](http://CABAR.asia) и узнайте, хорошо ли вы знаете, как защитить себя в интернете и что делать, если вас взломали?

**Вы – президент  
независимой страны.  
Недавно источники  
сообщили, что ваши  
аккаунты в  
социальных сетях  
хотят взломать и  
скомпрометировать  
вас. Вы решили, что  
доверять окружению  
нельзя и забрали  
под свой контроль**

**все личные  
аккаунты. Что  
делать дальше?**

**Чтобы сменить пароли,  
нужно придумать  
новые. Помощники  
советуют вам создать  
пароль, связанный с  
чем то ценным, чтобы  
не забыть. Например,  
«Майбах», «Мальдивы»,**

**«Доллар» или любимые  
цифры. Как поступите?**

**Вы зашли на сайт одной  
из социальных сетей,  
чтобы изменить пароль.  
Но кажется, в ней что-  
то не так. В адресе  
вместо .com написано  
.net. Помощники  
говорят, что всё  
нормально, так и  
должно быть. Какие**

**следующие действия?**

**Вы вспомнили запись прослушки в кабинете во время службы вашего предшественника. На ней его советник по электронной безопасности говорил о какой-то двухфакторной аутентификации. Вы звоните в тюрьму, чтобы узнать у бывшего**

**президента, что это  
такое, надеюсь, что он  
поможет. Ведь вы были  
близкими друзьями. На  
другом конце вам  
отвечают:**

**Пароли везде сменили,  
теперь можно и страной  
заняться. Вы  
открываете свою  
электронную почту,  
чтобы проверить**

**корреспонденцию. Вам  
пришло сообщение на  
первый взгляд от  
президента соседней  
страны, где он просит  
перейти по ссылке. При  
этом вы заметили  
ошибку в имени –  
вместо буквы “и” стоит  
“е”. Перейдёте?**

**Рабочий день закончился.  
Вы сделали очень много дел  
и со спокойной душой**



**решили поехать в свой загородный дом, чтобы отдохнуть. Дорога долгая и, чтобы скоротать время, вы захотели поиграть на телефоне в свою любимую игру “Монополию”.**

**Потянувшись за телефоном в карман вы его не обнаруживаете. Проверив все карманы вы понимаете, что забыли его на рабочем столе.**

**Вы просите помощника найти**

**телефон и привезти его в  
загородный дом. Когда  
спустя долгое время  
помощник приехал и передал  
телефон, вы заметили, что  
он разблокирован. Что  
будете делать?**

**Вы еще раз сменили  
пароли и проверили  
свой телефон. Вроде  
всё хорошо. К вам  
подходит ваш внук и  
просит дать поиграть**

**на телефоне в новую  
игру под названием  
“Мафия”. Вы  
устанавливаете для  
внука эту игру, но она  
просит доступ к  
подозрительно большому  
количеству разрешений.  
Разрешить?**

**Вы отлично защитили  
все свои аккаунты.  
Спустя несколько дней**

**К вам в кабинет  
забегает секретарь и  
со страхом в глазах  
говорит, что ее  
аккаунты взломаны, а  
злоумышленники хотят  
опубликовать вашу с  
ней личную переписку.  
Восстановить пароли не  
получается, так как  
все резервные способы  
не работают. Что  
делать?**

# Ого! Как вас еще не взломали?!

Скорее всего с таким уровнем безопасности, вас взломают в считанные секунды. Надеемся, этот тест поможет вам сохранить свои данные и чувствовать себя спокойнее.

Используйте приватный режим на чужих компьютерах. С его помощью можно не выходить вручную из каждой социальной сети, достаточно просто закрыть браузер – авторизация сбросится, а пароли не сохранятся.

Используйте пароли для разблокировки телефона и учётных записей на компьютере.

Специалисты по защите данных говорят, что разблокировка по отпечатку пальцев не лучшая идея, особенно Face ID. Например, полиция может просто взять ваш палец или поднести телефон к лицу.

Шифруйте и блокируйте приложения и документы на устройствах. У всех телефонов есть встроенная функция блокировки приложения отдельным паролем. Также используйте шифрование телефона, эта функция есть у всех современных устройств. Найти ее можно в настройках.

Этот способ поможет защитить ваши данные при потере телефона или в случае его кражи.

# **Неплохо! Но достаточно ли ЭТИХ знаний, чтобы защитить себя?**

У вас хорошие знания о кибербезопасности, но есть чему поучиться. Надеемся, что знания, полученные во время прохождения этого теста помогут вам.

Используйте приватный режим на чужих компьютерах. С его помощью можно не выходить вручную из каждой социальной сети, достаточно просто закрыть браузер – авторизация сбросится, а пароли не сохранятся.

Используйте пароли для разблокировки телефона и учётных записей на компьютере.

Специалисты по защите данных говорят, что разблокировка по отпечатку пальцев не лучшая идея, особенно Face ID. Например, полиция может просто взять ваш палец или поднести

телефон к лицу.

Шифруйте и блокируйте приложения и документы на устройствах. У всех телефонов есть встроенная функция блокировки приложения отдельным паролем.

Также используйте шифрование телефона, эта функция есть у всех современных устройств. Найти ее можно в настройках. Этот способ поможет защитить ваши данные при потере телефона или в случае его кражи.

# **Поздравляем! Вы практически гуру в мире кибербезопасности!**

Ваши личные данные за семью замками, но не расслабляйтесь. Злоумышленники постоянно ищут новые методы взлома, поэтому будьте начеку.

Используйте приватный режим на чужих компьютерах. С его помощью можно не выходить вручную из каждой социальной сети, достаточно просто закрыть браузер – авторизация

сбросится, а пароли не сохранятся.

Используйте пароли для разблокировки телефона и учётных записей на компьютере.

Специалисты по защите данных говорят, что разблокировка по отпечатку пальцев не лучшая идея, особенно Face ID. Например, полиция может просто взять ваш палец или поднести телефон к лицу.

Шифруйте и блокируйте приложения и документы на устройствах. У всех телефонов есть встроенная функция блокировки приложения отдельным паролем.

Также используйте шифрование телефона, эта функция есть у всех современных устройств. Найти ее можно в настройках. Этот способ поможет защитить ваши данные при потере телефона или в случае его кражи.