Ежемесячный журнал по вопросам компьютерной безопасности

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Сильные пароли: парольные фразы
- Безопасное использование паролей
- Ресурсы

Пароли

Обзор

Одним из основных способов удостоверения нашей личности является использование пароля. Например, для входа в электронную почту, банковскую учетную запись или совершения онлайн покупок с помощью таких устройств, как ноутбук или смартфон. Во многих случаях, пароль – это ключ в ваше королевство. Поэтому, если кто-то получит ваш пароль, то он сможет украсть вашу идентификацию, перевести деньги или получить всю вашу конфиденциальную информацию. Давайте поговорим о том, как сделать пароль сильным и как его использовать безопасно.

Об авторе

Рауль Сайлес – автор майского выпуска OUCH! Рауль основатель и старший аналитик по безопасности компании Taddong. Он также автор публикаций и инструктор в сфере информационной безопасности. Больше информации о Рауле можно найти в Twitter **@taddong** или в его блоге **http://blog.taddong.com/**.

Сильные пароли: парольные фразы

Киберпреступники разрабатывают сложные программы, которые могут подбирать или «грубо взламывать» ваши пароли, и они постоянно совершенствуют эти программы. Это значит, что ваши пароли могут взломать, если они лёгкие или их легко подобрать. Никогда не используйте распространённую информацию в ваших паролях, такую, как дата рождения, имя питомца или что-нибудь подобное, что легко можно найти в социальных сетях или в Google. Вместо этого создайте сильный пароль, который будет длинным, и чем больше символов в нём, тем лучше. Например, вместо одного слова используйте несколько или даже целое предложение. Такого рода пароли называются парольными фразами, и это один из самых лучших способов создать сильный пароль. Рассмотрим один из примеров, как это сделать:

time for my coffee

Это всё, что вам нужно. Если нужно, вы можете усилить пароль с помощью дополнительных символов, заглавных букв или чисел, как на примере ниже. Это особенно важно, если вы заходите на сайт, не позволяющий использовать несколько слов или предложение в качестве пароля:

Пароли

Time f0r my coffee!

Это пример того, как можно использовать заглавные буквы. Также вы можете заменить буквы цифрами или символами, например, заменить букву «а» на символ «@», букву «о» на символ ноль, или использовать знаки пунктуации, такие, как знак вопроса, точка и даже пробел. Если веб сайт или программа ограничивает количество символов, используйте максимально допустимое количество.

используйте сильные пароли, предпочтительно парольные фразы из нескольких слов и соблюдайте осторожность

Безопасное использование паролей

Кроме использования сильных паролей, необходимо знать о мерах безопасности их использования. Просто иметь сильный пароль недостаточно, если плохие парни его похитят или скопируют.

1. Убедитесь, что используете различные пароли для различных учетных записей. Например, никогда не используйте рабочий пароль или пароль банковского аккаунта как пароль для личного аккаунта социальных сетей, таких как Facebook, YouTube или Twitter. В этом случае, если один из паролей взломают, другие аккаунты будут в безопасности. Если у вас слишком много паролей и их сложно запомнить, используйте менеджер паролей. Это специальная программа, которая запускается на компьютере или мобильном устройстве и безопасно хранит все ваши пароли. Вам нужно будет запомнить только пароль вашего компьютера и этой программы. Если ваши пароли для рабочих аккаунтов, уточните у руководства или в службе поддержки, разрешено ли использование программы менеджера паролей в вашей организации.

2. Никогда и никому не сообщайте ваши пароли, в том числе коллегам. Помните, ваш пароль – это секрет, если кто-нибудь ещё его знает, то это уже не секрет. Если вам пришлось кому-то сообщить свой пароль или вы подозреваете, что его могли узнать или украсть, немедленно смените пароль.

3. Не пользуйтесь публичными компьютерами, например, в библиотеках или гостиницах, для входа в рабочий или банковский аккаунт. Поскольку кто угодно может пользоваться этими компьютерами и заразить их вредоносными вирусами, которые запоминают каждое нажатие клавиши. Заходите в рабочий или банковский аккаунт только с надёжных компьютеров или устройств.

Пароли

4. Будьте осторожны с сайтами, которые требуют ответа на персональные вопросы. Ответы на эти вопросы могут понадобиться для восстановления забытых паролей. Проблема в том, что ответы на эти вопросы можно найти в Интернет или даже на странице Facebook. Убедитесь, что при ответе на эти вопросы вы используете недоступную общественности информацию или даже её выдумали. Менеджер паролей поможет сохранить дополнительные данные.

5. Многие онлайн аккаунты предлагают так называемую двухфакторную аутентификацию или двухступенчатую проверку. В этом случае вам нужно не только ввести пароль, но и получить код на смартфон. Такая опция обеспечивает лучшую защиту, чем просто пароль. По возможности, используйте этот более сильный метод аутентификации.

6. Мобильные устройства часто запрашивают PIN для доступа. Помните, что PIN и есть пароль. Чем длиннее PIN, тем более он безопасен. На практике, в большинстве устройств можно изменить PIN на реальный пароль.

7. И, наконец, если вы больше не используете аккаунт, убедитесь, что закрыли его, удалили или заблокируйте.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Дополнительная информация

2-шаговая верификация:	http://www.google.com/landing/2step
Менеджеры паролей:	http://www.freepasswordmanager.com
Как создать надежный пароль:	http://preview.tinyurl.com/d6xq77k
Проверка надёжности пароля:	http://preview.tinyurl.com/d2f2ssn
Безопасные пароли:	http://preview.tinyurl.com/ct4opb6
Онлайн генератор паролей:	http://genpas.narod.ru
Сильные пароли:	https://xkcd.com/936
Термины по информационной безопасности:	http://preview.tinyurl.com/6wkpae5
Ежедневные советы Института SANS:	http://preview.tinyurl.com/6s2wrkp

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова