Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

Паролевые фразы

Обзор

Мы используем пароли в повседневной жизни для входа в электронную почту, банковский аккаунт, для онлайн покупок или доступа к смартфону.

Но пароли являются и нашей слабой стороной: если кто-то их узнает или украдет, то получит доступ к деньгам или личной информации. Сильный пароль обеспечит вам надежную защиту. В этом выпуске мы поговорим о том, как создать сильный пароль, который легко запомнить, т.е. использовать паролевые фразы.

Об авторе

Гай Бруно - старший консультант компании IPSS Inc., инструктор Института SANS и управляющий ISC (Internet Storm Center). Гай имеет сертификацию SANS GSE и прошел обучение по программе SANS Cyber Guardian. Гай ведет записи в Twitter **@GuyBruneau** и **handlers.sans.org/gbruneau**.

Паролевые фразы

Проблема заключается в том, что злоумышленники создают и совершенствуют все более сложные методы подбора или взлома паролей. И они постоянно совершенствуют эти методы. Это значит, что если ваши пароли слабые, то они с легкостью могут их взломать или подобрать. Важным шагом для защиты является использование надёжных паролей. Чем больше символов в вашем пароле, тем сложней его подобрать. Однако сложные длинные пароли сложней запомнить. Поэтому, вместо большого количества символов мы рекомендуем использовать ключевые фразы или предложения, которые легко запомнить, но трудно взломать. Например:

Where is king Julian?

Эта фраза сильна не только потому, что состоит из 21 символа, но и включает заглавные буквы и символы (помните, пробелы и знаки препинания тоже являются символами). Вы можете сделать свой пароль ещё сильнее, если замените буквы «а» на символ @ или буквы «о» на цифру 0. Если веб сайт или программа ограничивает количество символов пароля, используйте максимально возможное.

Безопасное использование паролевых фраз

При использовании паролевых фраз тоже следует соблюдать осторожность, ведь плохие парни тоже могут её скопировать или украсть.

Паролевые фразы

Использование паролевых фраз – один из самых эффективных шагов, который вы можете предпринять для защиты своей личности и информации.

1. Используйте разные пароли для разных учётных записей и устройств. Никогда не используйте пароль или паролевые фразы аккаунтов социальных сетей (например, Facebook, YouTube или Twitter) для рабочих или банковских аккаунтов. В случае взлома одного из аккаунтов, другие останутся в безопасности. Если у вас большое количество паролей и их сложно запомнить, что довольно часто встречается, используйте менеджер паролей. Это специальная программа, которая хранит все ваши паролевые фразы. Таким образом, вам придется запомнить всего лишь паролевые фразы к компьютеру и менеджеру паролей.

2. Никому не сообщайте свои паролевые фразы или свою стратегию их создания, включая коллег. Помните, паролевая фраза – это тайна и если кто-то ещё её знает, то это уже не безопасно. Если вы случайно поделились своей паролевой фразой или считаете, что её узнали, поменяйте её как можно скорей.

3. Также как и пароли, паролевые фразы не стоит выбирать из хорошо известных фраз, например, фраза “Four score and seven years ago” не подходит для паролевой фразы, так как слишком известна.

4. Не входите в рабочие или банковские аккаунты с публичных компьютеров в библиотеке или гостинице. Эти компьютеры доступны всем и могут быть заражены вирусами, перехватывающими нажатия клавиш. Используйте для работы или банковских операций только проверенные мобильные устройства или компьютеры.

5. Будьте осторожны с сайтами, запрашивающими ответы на конфиденциальные вопросы. Эти вопросы часто используют для восстановления и сброса паролей. Проблема в том, что ответы на эти вопросы зачастую можно найти в Интернете или на странице Facebook. Убедитесь, что даёте информацию, которой нет в публичном доступе или придумайте её сами. Менеджер паролей поможет вам сохранить эту дополнительную информацию.

6. Многие интернет аккаунты предлагают двухфакторную аутентификацию или двухступенчатую проверку. В этом случае, кроме паролевой фразы нужно будет ввести ещё код, который вам отправят на смартфон.

Паролевые фразы

Эта опция обеспечивает более надежную защиту, чем использование паролевой фразы. По возможности, используйте двухфакторную аутентификацию.

7. Мобильные устройства часто запрашивают ПИН код для защиты доступа к ним. Помните, что ПИН код – это тоже пароль. Чем ПИН код длиннее, тем он безопасней. Многие устройства позволяют заменить цифры ПИН кода на паролевую фразу.

8. И, наконец, если вы не пользуетесь аккаунтом, закройте, удалите или заблокируйте его.

Общественные ресурсы

Не пользуйтесь общественными компьютерами, например, в лобби отелей, библиотеках или интернет-кафе. Вы же не знаете, кто пользовался этим компьютером до вас, компьютеры могут быть заражены вирусами случайно или специально. По возможности, используйте только свое устройство для соединения с Интернетом. Если возникнет необходимость воспользоваться публичным компьютером, то постарайтесь не пользоваться сервисами, требующими вводить логин и пароль.

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.

Ресурсы

Двухступенчатая Верификация:	http://www.securingthehuman.org/ouch/2013#august2013
Менеджер паролей:	http://www.securingthehuman.org/ouch/2013#october2013
Социальная инженерия:	http://www.securingthehuman.org/ouch/2014#november2014
Термины по Информационной безопасности:	http://www.securingthehuman.org/resources/security-terms

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

