Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

Парольные фразы

Введение

Об авторе

Ми-Нон Нгуен - сертифицированный инструктор Института SANS и CEO - Ведущий консультант компании Secured IT Solutions. Она имеет несколько престижных сертификаций и более 14 лет опыта разработки, совершенствования и руководства проектами по информационной безопасности в различных отраслях. Блог в Twitter: **@MenopN** и страница в LinkedIn: My-Ngoc «Menop» Nguyen

Пароли – это то, что мы используем почти ежедневно для получения доступа к электронной почте, онлайн банкинга, онлайн покупок или доступа к смартфону. Но пароли являются одним из наших уязвимых мест: если кто-то узнает или угадает ваш пароль, то сможет перевести деньги с вашего счёта, прочитать вашу электронную почту или украсть ваши паспортные данные. Вот почему сильные пароли так важны для защиты вашей информации. Сложные пароли смущают тем, что их сложно запомнить и напечатать. В этом выпуске мы поговорим о том, как создать сильные пароли, которые легко запомнить, так называемые парольные фразы.

Парольные фразы

Мы столкнулись с тем, что кибер преступники разработали технически сложные и эффективные методы грубого взлома (автоматического подбора) паролей. Это значит, что злоумышленники могут взломать ваш пароль, если он слабый или его легко угадать. Одним из самых важных шагов защиты является использование сложных паролей. Обычно это заключается в создании сложных паролей; однако их сложно запомнить и сложно печатать. Поэтому мы рекомендуем использовать парольные фразы – набор случайных слов или предложение. Чем больше символов содержит парольная фраза, тем она сильнее. Преимущество заключается в том, что их очень легко запомнить и напечатать, а злоумышленникам сложно взломать. Вот два примера:

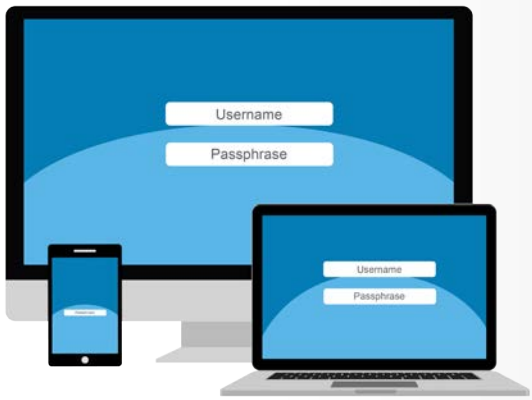
Sustain-Easily-Imprison (Легко-Перенести-Тюрьму)

Time for tea 1:23 (Время Для Чая 1:23)

Эти пароли сильные не только из-за количества символов, но и из-за использования заглавных букв и знаков

Парольные фразы

(помните, знаки пунктуации и пробелы тоже символы). В то же время, эти парольные фразы довольно легко запомнить и напечатать. Вы можете сделать эти пароли ещё сильней, если замените буквы «а» знаками «@» или буквы «о» нулями. Если сайт или программа ограничивает количество символов пароля, то следует использовать максимально разрешённое.



Парольные фразы – самый простой способ создать и запомнить сложные пароли.

Безопасное использование парольных фраз

Используйте парольные фразы с осторожностью. Использование парольной фразы не поможет, если злоумышленники могут украсть или скопировать ваш пароль.

1. Используйте различные парольные фразы для каждой учётной записи или устройства. Например, не следует использовать один и тот же пароль для персонального аккаунта, такого как Facebook, YouTube или Twitter, и банковского или служебного. В случае, если один из аккаунтов взломают, все остальные будут по-прежнему в безопасности. Если вам сложно запомнить столько парольных фраз одновременно (что вполне вероятно), используйте менеджер паролей. Это специальная программа, которая помогает безопасно хранить пароли. В этом случае вам придётся запомнить только пароль к устройству и к этой программе.
2. Никому не говорите свои парольные фразы и даже принципы их создания, включая коллег или руководителей. Помните, что парольная фраза должна быть секретом, а если кто-то ещё её знает, то это уже не секрет. Если вы случайно проговорились или у вас есть хоть малейшее подозрение, что пароль украли, смените его немедленно. Пароль можно сообщить только членам семьи на непредвиденный случай. Для этого парольную фразу следует записать (убедитесь, что она не совпадает с рабочей) и положить в безопасное место, а это место сообщить члену семьи. Если с вами что-то случится, ваш любимый человек сможет получить доступ к важным аккаунтам.
3. Никогда не используйте общественные компьютеры, например, в гостиницах или интернет кафе, для доступа к важным аккаунтам. Учитывая, что они доступны многим, на них может быть вирус или программа, записывающая каждое нажатие клавиш. Загружайтесь только с проверенного компьютера или мобильного устройства.

Парольные фразы

4. Будьте осторожны с сайтами, которые запрашивают ответы на личные вопросы. Эти ответы могут использоваться для восстановления пароля, если вы его забудете. Но проблема в том, что ответы на некоторые вопросы легко можно найти в Интернете или даже на вашей страничке Facebook. Убедитесь, что вы используете какой-либо из этих вопросов, ответ на который нельзя найти в ваших публикациях или придумайте его. Не можете запомнить ответы на все эти вопросы? Выберите какого-нибудь героя из фильма и ответьте на вопросы от его имени. Второй вариант: используйте менеджер паролей для хранения этих дополнительных данных.
5. Многие сайты предлагают двухступенчатую аутентификацию, или верификацию. В этом случае, при входе в аккаунт вам потребуется ещё один пароль, который придёт на ваш смартфон. С этой функцией безопасность аккаунта намного выше, чем с парольной фразой. Всегда старайтесь использовать усиленные методы аутентификации.
6. В большинстве мобильных устройств можно настроить доступ через PIN код. Помните, что это всего лишь пароль. И чем он длинней, тем более безопасный. Большинство устройств позволяют изменить пароль на более сложный или даже использовать биометрические данные, такие как отпечатки пальцев.
7. Если вы не используете аккаунт, то его следует закрыть, удалить или сделать неактивным.

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 securingthehuman.sans.org/ouch/archives.

Ресурсы

Менеджеры паролей:	https://securingthehuman.sans.org/ouch/2015#october2015
Двухступенчатая верификация:	https://securingthehuman.sans.org/ouch/2015#september2015
Защити свой аккаунт:	https://lockdownyourlogin.com
Курс Института SANS SEC301 – Основы Информационной Безопасности:	https://sans.org/sec301

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли
Русский перевод: Александр Котков, Ирина Коткова

