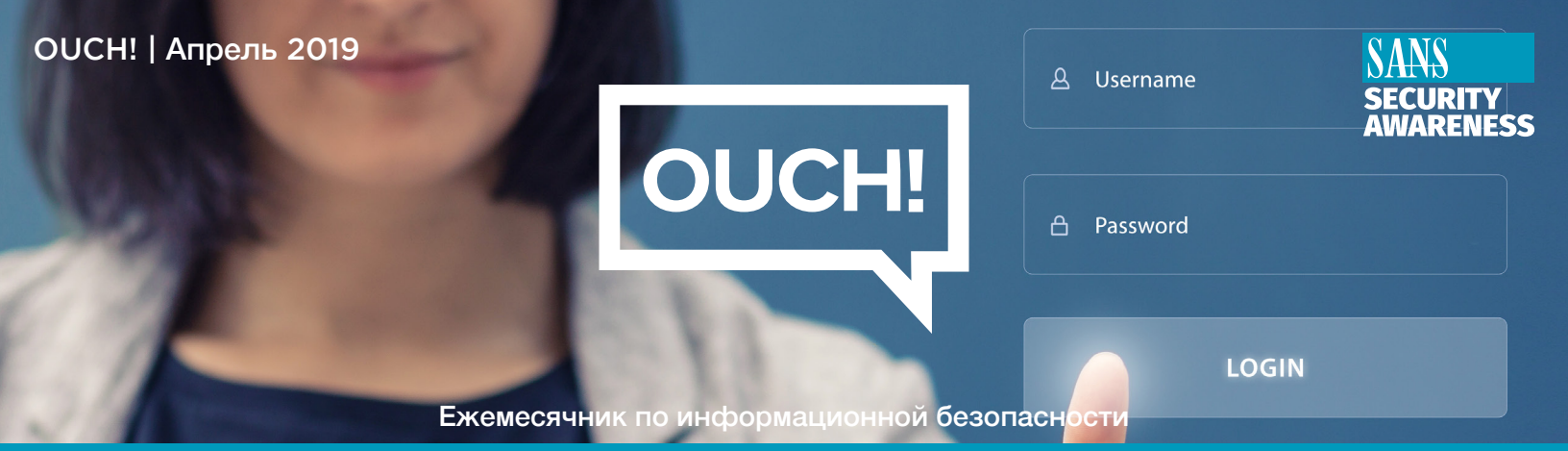

SANS SECURITY AWARENESS

OUCH!

Ежемесячник по информационной безопасности

Создание паролей

Обзор

Вам часто говорят, что ваши пароли являются ключом к защите ваших учетных записей (и это правда!), но редко вам предоставляется простой способ безопасного создания и управления всеми вашими паролями. Ниже мы рассмотрим три простых шага, чтобы упростить ваши пароли, заблокировать ваши учетные записи и защитить ваше будущее.

Парольные фразы

Дни безумно, сложных паролей прошли. Такие пароли трудно запомнить, сложно набрать, а современные суперскоростные компьютеры кибер-злоумышленники могут легко взломать. Главное в паролях - сделать их длиннее, чем больше символов, тем лучше. Они называются парольными фразами, типом надежного пароля, который использует короткое предложение или случайные слова. Вот два примера

Время крепкого кофе!
потерянная-улитка-ползет-пляж

Оба они сильны с более чем двадцатью символами, легко запоминаются и просты для ввода, их трудно взломать. Вы столкнетесь с веб-сайтами или ситуациями, требующими добавления символов, цифр или заглавных букв к вашему паролю, и это нормально. Помните, что длина является наиболее важной.

Менеджеры паролей

Вам нужен надежный пароль для каждой учетной записи. Если вы повторно используете один и тот же пароль для нескольких учетных записей, вы подвергаете себя большой опасности. Всё, что нужно кибер-злоумышленнику - это взломать веб-сайт который вы используете, украсть все пароли, в том числе и ваш, а затем использовать свой пароль для входа во все ваши учетные записи, от вашего имени. Это происходит гораздо чаще, чем вы думаете. Не верите этому? Проверьте сайт www.haveibeenpwned.com, чтобы узнать , какие сайты вы используете, возможно они были взломаны и пароли могли быть подвергнуты риску. Итак, что нужно делать? Используйте менеджер паролей.

Это специальные компьютерные программы, которые надежно хранят все ваши пароли в зашифрованном хранилище. Вам нужно запомнить только один пароль для вашего менеджера паролей. Менеджер паролей автоматически

извлекает ваши пароли всякий раз, когда они вам нужны, и регистрирует вас на веб-сайтах. Они также имеют другие функции, такие как хранение ваших ответов на секретные вопросы, предупреждая вас при повторном использовании паролей, генератор паролей, гарантирует использование надежных паролей, и многие другие функции. Большинство менеджеров паролей также надежно синхронизируются практически с любым компьютером или устройством, поэтому независимо от того, какую систему вы используете, у вас есть простой и безопасный доступ ко всем вашим паролям.

Наконец, обязательно запишите пароль от своего менеджера паролей и храните его в безопасном месте дома. Некоторые менеджеры паролей даже позволяют распечатать восстановления менеджера паролей. Таким образом, если вы забудете пароль для вашего менеджера паролей, у вас есть резервная копия. Или, если вы заболели или оказались в чрезвычайной ситуации, ваш супруг или член семьи, которому вы доверяете, может получить информацию от вашего имени.

Двухэтапная проверка

Двухэтапная проверка (часто называемая двухфакторной аутентификацией или многофакторной аутентификацией) добавляет дополнительный уровень безопасности. При входе в учетные записи требуется две вещи: пароль и цифровой код, который генерируется вашим смартфоном или отправляется на ваш телефон. Этот процесс гарантирует, что даже если злоумышленник получит ваш пароль, он все равно не сможет попасть в ваши учетные записи. Двухэтапная проверка проста в настройке, и вам обычно нужно использовать ее только один раз при входе в систему с нового компьютера или устройства. Включите эту опцию, когда это возможно, особенно для наиболее важных счетов, таких как банк или пенсионные счета или доступ к вашей электронной почте. Если вы используете менеджер паролей, мы настоятельно рекомендуем защитить его надежной парольной фразой и двухэтапной проверкой.

Это может звучать глупо, но эти три простых шага имеют большое значение для защиты вашей работы, репутации и вашего финансового будущего.

Приглашенный редактор

Джастин Хендерсон *(@SecurityMapper) является соучредителем H & A Security Solutions, сертифицированного института инструкторов SANS и автора курсов SANS Cyber Defense и SIEM. Его интересует все, что связано с киберзащитой. Он консультирует уже пятнадцать лет.*

Ресурсы

Я был взломан:	https: //haveibeenpwned.com/
Сайт двухфакторной аутентификации:	https: //twofactorauth.org/
NIST SP800-63B Руководство по цифровой идентификации:	https: //pages.nist.gov/800-63-3/sp800-63b.html/
Плакат: Вы являетесь мишенью:	https://www.sans.org/u/OGi

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:* www.sans.org/security-awareness/ouch-newsletter. *Редакция: Уолт Скривенс, Фил Хоффман, Алэн Вэггонер, Шерил Конли*