Ежемесячный журнал по вопросам компьютерной безопасности

OUCH!

В ЭТОМ ВЫПУСКЕ…

Менеджер паролей

Проблема

Чаще всего, одним из основных моментов для защиты персональной информации, является использование сильных паролей. Сильным можно назвать пароль, который сложно подобрать или взломать специальной хакерской программой. Закономерность следующая: чем длинней и сложней пароль, тем он сильнее и безопасней. Но такой пароль нелегко запомнить. В результате чего люди часто используют один и тот же сложный пароль или с небольшими вариациями для различных аккаунтов, приложений и устройств. Ещё большей опасности подвергаются те, кто используют один и тот же пароль для рабочих и личных аккаунтов. Если вы один из них, то сильно рискуете. Однажды взломав ваш пароль, киберпреступники потенциально получают доступ ко всем вашим аккаунтам. Все, что вам нужно – это использовать сильный и уникальный пароль для каждого аккаунта. Даже если кто-то получит доступ к одному из аккаунтов, все остальные по-прежнему будут в безопасности. К сожалению, проблема в том, что практически никто не сможет запомнить все эти пароли ко всем своим устройствам и аккаунтам.

Об авторе

Джордж Бэйкс - Технический директор отдела Intelligence & Response компании Northrop Grumman и сертифицированный инструктор SANS с 2001 года. Джордж будет читать в ноябре в Лондоне курс Security 502, защита периметра.

Решение

Некоторые записывают свои пароли на листке бумаги или, хуже того, приклеивают листок с паролями на монитор компьютера (скорее всего, вы видели в окнах офисных зданий мониторы, обклеенные стикерами). Такой способ хранения паролей нельзя назвать безопасным, так как любой может получить пароль, вы можете их потерять в дороге или их могут украсть. Соответственно, нам нужен безопасный способ хранения всех паролей в одном месте. Лучше всего использовать программу, которая будет автоматически вводить пароли, и загружаться на сайты и приложения. А ещё лучше использовать программу, которая будет генерировать сложные пароли, и хранить конфиденциальную информацию, например, по кредитным картам.

Менеджер паролей

К счастью, такая программа существует и называется Менеджер Паролей (или Хранилище Паролей).

Использование менеджера паролей - это простой способ безопасного хранения уникальных паролей для каждой из ваших учетных записей.

Как работает менеджер паролей

Менеджер паролей похож на виртуальный сейф. Прежде всего, вам нужно установить виртуальный сейф в виде программы на ваш компьютер или мобильное устройство. Затем он соберёт все ваши логины и пароли, зашифрует их и будет хранить на устройстве или на облаке. Затем к этой базе данных нужно создать всего один пароль. В этом случае вам придется запомнить всего один пароль, пароль для менеджера паролей. Когда вам понадобятся учетные данные, например, для входа в банковский аккаунт или электронную почту, вы просто введёте пароль для менеджера паролей. Это решение позволяет создавать уникальный пароль для каждого аккаунта, даже если у вас их сотни, без необходимости их запоминать и даже видеть. Так как менеджер паролей хранит все конфиденциальные данные, то вы должны использовать очень сильный пароль к нему и всегда его помнить.

Большинство современных менеджеров паролей могут интегрироваться с вашим браузером. Это позволит автоматически авторизоваться с помощью менеджера паролей при входе на сайт, например, интернет-магазина. Даже если вы поменяете пароль к этому сайту, менеджер паролей тоже обновит данные. Некоторые менеджеры паролей работают и на мобильных устройствах, но большинство не совместимы с мобильными приложениями, только с вашим браузером на устройстве.

Как правильно выбрать менеджер паролей

Существует огромное количество бесплатных и платных менеджеров паролей. Когда будете выбирать, придерживайтесь следующих советов:

Менеджер паролей

- Выбирайте решения известных и надёжных производителей. Остерегайтесь решений, которые только что появились и о них очень мало отзывов пользователей или их нет. Киберпреступники могут создавать фальшивые программы для кражи данных.
- Убедитесь, что программа, которую вы выбрали, регулярно исправляется и обновляется. Следует использовать самую последнюю версию.
- Программа должна быть вам понятна и проста в использовании. Если она слишком сложная, то высока вероятность неправильного использования.
- Пароли следует шифровать, придерживаясь стандартов компании. Будьте осторожны с программами, которые используют собственные или неизвестные стандарты шифрования.
- Программа должна работать на всех ваших компьютерах. Некоторые продвинутые версии совместимы с мобильными устройствами.
- Полезной функцией является синхронизация ваших устройств. Если программа поддерживает эту функцию, то она должна шифровать данные до отправки на центральную систему.
- Программа должна предоставлять возможность создавать произвольные пароли и помогать отслеживать сроки их действия.
- Программа должна определять насколько сильный пароль вы выбрали.

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

Обзор Менеджеров Паролей:	http://www.pcmag.com/category2/0,2806,2403435,00.asp
Должен ли я поменять свой пароль?	https://shouldichangemypassword.com/all-sources.php
Ежедневные советы Института SANS:	https://www.sans.org/tip_of_the_day.php
Популярные менеджеры паролей в сравнении:	http://habrahabr.ru/post/125248/

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