Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

Менеджеры паролей

Обзор

Лучшее, что вы можете сделать для своей защиты онлайн - использовать уникальный и сильный пароль для каждой учётной записи. К сожалению, у большинства из нас так много аккаунтов, что запомнить все пароли практически невозможно. Простое решение этой проблемы – использовать менеджер паролей (иногда его называют «хранилище паролей»). Эти приложения специально созданы для безопасного хранения учетных данных. Кроме того, с их помощью вход на веб сайты, мобильные и другие приложения становится намного проще.

Об авторе

Ленни Зельцер обеспечивает информационную безопасность клиентов компании NCR Corp. Он также преподает в Институте SANS для профессионалов в области информационной безопасности. Ленни ведет записи в Twitter **@lennyzeltser** и публикует статьи на сайте **zeltser.com**.

Как работают менеджеры паролей

Менеджер паролей выполняет функцию электронного сейфа для логинов, паролей и другой конфиденциальной информации. Когда интернет сайт запрашивает логин и пароль для входа в аккаунт, менеджер паролей может автоматически вводить ваш пароль и выполнять безопасный вход на сайт. С его помощью легко можно иметь сотни уникальных и сильных паролей и вам не придётся их запоминать.

Менеджер паролей хранит информацию в базе данных, которую называют хранилищем. Менеджер паролей шифрует содержимое хранилища и защищает его мастер-паролем, известным только вам. Когда вам нужно получить пароль для входа в онлайн банкинг или электронную почту, вы просто вводите мастер-пароль к менеджеру паролей и получаете доступ к хранилищу.

Некоторые менеджеры паролей хранят данные непосредственно на компьютере или в смартфоне, другие - на удалённых сайтах компаний-разработчиков этих программ. Кроме того, многие менеджеры паролей могут автоматически синхронизировать содержимое хранилища между несколькими вашими устройствами. В этом случае, при обновлении пароля на ноутбуке, пароль обновится и на смартфоне, планшете или других устройствах, которыми вы пользуетесь. Но независимо от того, где хранятся данные, это приложение необходимо установить на всех устройствах, где вы будете использовать менеджер паролей.

Менеджеры паролей

При первом использовании вам необходимо вручную ввести или импортировать все логины и пароли. После этого, менеджер паролей будет распознавать регистрацию новых аккаунтов и обновление паролей на существующих аккаунтах, автоматически фиксируя изменения в хранилище. Эта функция возможна, потому что большинство менеджеров паролей интегрируются с браузером. Это также позволяет программе автоматически выполнять вход на сайты.

Менеджеры паролей – простое решение для безопасного хранения и удобного использования всех ваших паролей.

Менеджер паролей специально создан для безопасного хранения вашей конфиденциальной информации. Поэтому следует защитить хранилище этой информации с помощью сильного и сложного мастер-пароля, который сложно угадать. На практике, мы рекомендуем использовать паролевую фразу, один из самых надёжных типов паролей. Если ваш менеджер паролей поддерживает двухступенчатую верификацию, ей следует воспользоваться. Наконец, убедитесь, что не используете этот пароль для других систем или аккаунтов. Тогда, в случае если хакерам удастся получить копию вашего хранилища паролей, они не смогут угадать пароль и получить доступ к содержимому хранилища. И последнее, мастер-пароль следует помнить. Если вы его забудете, то не сможете получить доступ к другим паролям.

Как выбрать менеджер паролей

Существует огромное количество бесплатных и коммерческих менеджеров паролей. При выборе нужно учитывать следующее:

- Убедитесь, что менеджер паролей будет работать на всех системах или мобильных устройствах, с которых вы будете использовать ваше хранилище паролей. Программа должна обеспечивать удобную синхронизацию содержимого хранилища между всеми вашими устройствами.
- Выбирайте только хорошо известные и надёжные менеджеры паролей. Остерегайтесь совсем новых продуктов, по которым мало или совсем нет отзывов. Подобно фальшивым антивирусам, кибер мошенники могут подделывать менеджеры паролей с целью кражи данных.
- Менеджер паролей должен быть простым в использовании. Если менеджер паролей слишком сложен для вас, следует поискать более простую альтернативу, соответствующую вашему опыту и потребностям.
- Какой бы вы не выбрали менеджер паролей, удостоверьтесь, что он активно обновляется. Всегда используйте самую последнюю версию.

Менеджеры паролей

- С помощью менеджера паролей вы легко можете использовать сильные пароли для различных аккаунтов, включая возможность автоматического генерирования сложных паролей и оценке их надёжности.
- Менеджер паролей даёт возможность хранить и другую конфиденциальную информацию, например, ответы на секретные вопросы, номера кредитных карт или номера участника бонусных программ авиакомпаний.
- Остерегайтесь менеджеров паролей, которые используют непроверенные или неизвестные методы шифрования; отдавайте предпочтения системам хранения данных со стандартным шифрованием. Если разработчик говорит, что они разработали свои уникальные методы шифрования, держитесь от них подальше.
- Не следует выбирать менеджеры паролей с функцией восстановления мастер-пароля. Это значит, что у них есть доступ к вашему мастер-паролю, а это значительно увеличивает риски.

Менеджеры паролей – отличное решение для хранения паролей и другой конфиденциальной информации. Поскольку они хранят очень важные данные, их следует защитить очень сильным паролем, который сложно подобрать злоумышленникам, но легко запомнить вам.

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

Паролевые фразы: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_ru.pdf

Двухступенчатая верификация: https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201509_ru.pdf

Top Five Password Managers: http://lifehacker.com/5529133/five-best-password-managers

Выбираем лучший менеджер паролей:

http://lifehacker.ru/2014/01/10/keepass-vs-dashlane-vs-lastpass-vybiraem-luchshij-menedzher-parolej/

Ежедневные советы Института SANS: http://www.sans.org/tip_of_the_day.php

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