Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

Мениджъри на пароли

Преглед

Една от най-важните стъпки, които можете да предприемете, за да се защитите онлайн, е да използвате уникална, силна парола за всеки от вашите акаунти и приложения. За съжаление, най-вероятно за вас е невъзможно да запомните всичките си различни пароли за всичките си различни профили. Ето защо толкова много хора използват повторно същата парола. За съжаление, повторното използване на една и съща парола за различни профили е опасно, защото след като някой компрометира паролата ви, същият човек вече може да получи достъп до всичките ви други акаунти, които използват една и съща парола. Едно лесно решение е да използвате мениджър на пароли, понякога наричан хранилище за пароли. Това са програми, които съхраняват сигурно всичките ви пароли, което улеснява поддържането на различна парола за всеки профил. Мениджърите на пароли правят това просто, защото вместо да се налага да запомните всичките си пароли, трябва само да запомните главната парола на вашия мениджър на пароли.

Гост-редактор

Крис Крисчънсън е консултант по сигурността на информацията, базиран в Калифорния, с 20 години опит и множество технически сертификати. Той е говорил на различни конференции и е допринесъл за много статии в индустрията. С Крис може да се свържете на **@cchristianson** и **https://ismellpackets.com**.

Как работят мениджърите на пароли

Мениджърите на пароли работят, като съхраняват всичките ви пароли в база данни, която понякога се нарича хранилище. Мениджърът на пароли криптира съдържанието на хранилището и го защитава с главна парола, която само вие знаете. Когато трябва да извлечете паролите си, като например да влезете в своето онлайн банкиране или имейл, просто въведете главната си парола в мениджъра си на пароли, за да отключите хранилището. В много случаи мениджърът на пароли автоматично ще изтегли паролата ви и ще ви я запише сигурно. Това прави лесно да имате стотици уникални, силни пароли, тъй като не е нужно да ги запомните.

Някои мениджъри на пароли съхраняват хранилището ви на компютъра или на мобилното ви устройство, докато други го съхраняват в облака. В допълнение, повечето мениджъри на пароли включват възможността за автоматично синхронизиране на съдържанието на вашето парола на няколко устройства, които вие упълномощите. По този начин, когато актуализирате парола на лаптопа си, тези промени биват синхронизирани с всичките ви други устройства. Независимо къде се съхранява базата данни, трябва да инсталирате приложението за управление

Мениджъри на пароли

на пароли на вашата система или устройство, за да го използвате.

Когато настройвате за първи път мениджър на пароли, трябва ръчно да въведете или импортирате вашите потребителски данни и пароли. След това мениджърът на пароли може да засече, когато се опитвате да се регистрирате за нов онлайн акаунт или да актуализирате паролата за съществуващ профил, като автоматично актуализирате хранилището. Това е възможно, защото повечето мениджъри на пароли работят ръка за ръка с вашия уеб браузър. Тази интеграция също така им позволява автоматично да влезете в уеб сайтове.

Мениджърите на пароли са лесен начин да съхранявате сигурно и да използвате всичките си различни пароли.

Важно е основната парола, която използвате, за да защитите съдържанието на мениджъра на пароли, да е силна и много трудна за отгатване. Всъщност ви препоръчваме да направите главната си парола фраза за достъп, която е един от най-силните видове пароли. Ако мениджърът ви за пароли поддържа потвърждаването в две стъпки, използвайте го за основната си парола. И накрая, не забравяйте да помните главната си парола. Ако я забравите, няма да имате достъп до някоя от другите си пароли.

Избор на мениджър на пароли

Има много мениджъри на пароли, от които можете да избирате. В секцията “Ресурси” предоставяме връзка към прегледи на мениджъри на пароли. Междувременно, когато се опитвате да намерите най-доброто за вас, имайте предвид следното:

- Мениджърът на пароли трябва да е лесен за използване. Ако откриете, че решението е твърде сложно за разбиране, намерете друго, което по-добре отговаря на вашия стил и опит.
- Мениджърът на пароли трябва да работи на всички устройства, на които има нужда да използвате пароли. Трябва също така лесно да можете да поддържате паролите си синхронизирани на всичките си устройства.
- Използвайте само добре известни и надеждни мениджъри на пароли. Бъдете предпазливи по отношение на продуктите, които не съществуват от дълго време или за които няма обратна връзка от общността. Кибер престъпниците могат да създадат фалшиви мениджъри на пароли, за да откраднат вашата информация. Също така бъдете много подозрителни към всеки производител, който твърди, че е разработил собствено решение за криптиране.
- Избягвайте всеки мениджър на пароли, който твърди, че може да възстанови главната ви парола. Това означава, че той знае главната ви парола, което ви излага на твърде голям риск.

Мениджъри на пароли

- Уверете се, че независимо от решението, което изберете, доставчикът продължава активно да го актуализира и да подобрява мениджъра на пароли, като се уверите, че винаги използвате най-новата версия.
- Мениджърът на пароли трябва да включва възможността автоматично да генерира силни пароли за вас и да ви покаже силата на паролите, които сте избрали.
- Мениджърът на пароли трябва да ви даде възможност да съхранявате други чувствителни данни, като например отговорите на вашите секретни въпроси за сигурност, кредитни карти или често срещани номера.

Мениджърите на пароли са чудесен начин за сигурно съхранение на всичките ви пароли и други чувствителни данни. Въпреки това, тъй като те защитават такава важна информация, не забравяйте да използвате уникална, силна главна парола, която не е само трудна за хакери, а лесна за запомняне.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на securingthehuman.sans.org/ouch/archives.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Ресурси

Топ мениджъри на пароли от 2017:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Фрази за достъп:	https://securingthehuman.sans.org/ouch/2017#april2017
Потвърждаване в две стъпки:	https://www.securingthehuman.org/ouch/2015#september2015
Заключете своите данни за достъп:	https://www.lockdownyourlogin.org/
SANS Съвет за сигурност на деня:	https://www.sans.org/tip-of-the-day

Редакторски колектив: Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли
Превод: Николай Дачев и Радослава Несторова