Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

Фрази за достъп

История

Гост-редактор

Ме Ноп Уин е сертифициран SANS инструктор и Главен инпълнителен директор/Главен консултант на Secured IT Solutions. Тя допринася знания и умения със своите топ сертификати и над 14 години развиване, усъвършенстване и управление на програми за кибер сигурност за различни индустрии и сектори. Twitter: **@MenopN** LinkedIn: My-Ngoc “Menop” Nguyen.

Паролите са нещо, които използвате почти всеки ден, от отварянето на имейла си или онлайн банкирането си, до купуването на стоки или отключването на смартфона си. Въпреки това, обаче, паролите са и една от най-слабите ви точки – ако някой научи или налучка паролата ви, той може да отваря сметките ви все едно сте вие, което би позволило прехвърлянето на парите ви, четенето на имейлите ви или присвояване на самоличността ви. Именно затова е изключително важно да имаме силни пароли, за да се защитим. Силните пароли, обаче, са обикновено объркващи, трудни за запомняне и трудни за въвеждане. В този бюлетин ще научите как да създавате силни пароли, които са лесни за запомняне и са лесни за изписване – те се наричат фрази за достъп.

Фрази за достъп

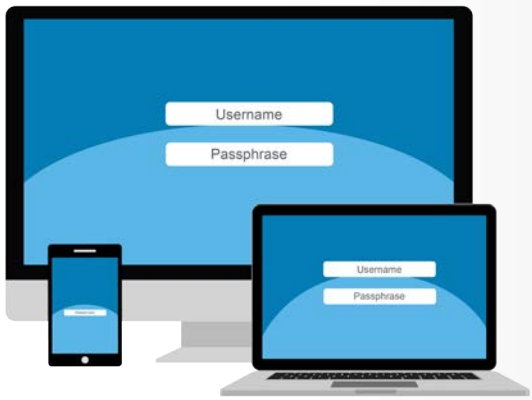
Предизвикателството пред което сме изправени всички ние е, че кибер хакерите са разработили изпипани и ефективни методи за разгадаване (автоматизирано отгатване) на пароли. Това значи, че лошите герои могат да компрометират паролите ви, ако са слаби или лесни за разгадаване. Важна стъпка за защитата ви е да използвате силни пароли. Обикновено това се прави чрез създаването на сложни пароли, които обаче могат да са трудни за запомняне, объркващи и трудни за изписване. Вместо това ви предлагаме да използвате фрази за достъп – серия от несвързани думи или изречение. Колкото повече символа има в паролата ви, толкова по-сложна е тя. Предимството е, че фразите са много по-лесни за запомняне и изписване, но са все така трудни за хакерите. Ето два примера:

Sustain-Easily-Imprison
Time for tea at 1:23

Това, което прави тези пароли толкова силни, не е просто фактът, че са много дълги, а това, че включват главни букви и символи (помнете, че интервалите и пунктуацята са символи). В същото врме, тези фрази за достъп са и лесни за помнене и изписване. Можете да направите фразата си за достъп още по-силна, ако желаете, като замените букти с цифри или символи, като замяната на буквата „а“ със символа „@“ или буквата „о“ с цифрата

Фрази за достъп

нула. Ако даден уебсайт или програма ограничава броя на символите, които използвате в паролата си, използвайте максималния брой позволени символи.



Фразите за достъп са по-прост начин да създадете и запомните силни пароли.

Сигурно използване на фразите за достъп

Трябва да бъдете внимателни и как използвате фразите за достъп. Използването на фраза за достъп няма да помогне, ако лошите герои могат лесни да я откраднат или копират.

1. Използвайте различна фраза за достъп за всеки акаунт или устройство, които имате. Например, никога не използвайте фраза за достъп за работа или за банковата си сметка, която е идентична на тази, която използвате за лични акаунти, като Facebook, YouTube или Twitter. По този начин, ако един от акаунтите ви бъде хакнат, другите ви акаунти ще останат защитени. Ако имате твърде много фрази за достъп, за да можете да помните всички (което е много често срещан проблем), обмислете използването на софтуер за управление на пароли. Това е специална програма, която съхранява безопасно всичките ви фрази за достъп. По този начин, единствените фрази за достъп, които трябва да използвате са тази за компютъра или устройството ви, както и тази за софтуера за управление на пароли.
2. Никога не споделяйте фразата си за достъп или стратегията си за създаването на такива с никого, включително колеги и мениджъри. Помнете, че фразата за достъп е тайна; ако някой знае фразата ви за достъп, то тя вече не е сигурна. Ако случайно споделите фразата си за достъп с някой друг или смятате, че фразата ви за достъп може да е била компрометирана или откраднатa, променете я веднага. Единственото изключение е, ако искате да споделите ключовите си лични фрази за достъп с много доверен член от семейството за спешни случаи. Един подход е да напишете личните си ключови фрази за достъп (уверете се, че не са свързани с работата ви), да ги поставите за съхранение на безопасно място и да споделите това място с доверен член от семейството. По този начин, ако нещо се случи с вас и имате нужда от помощ, вашите близки ще имат достъп до най-важните ви акаунти.
3. Не използвайте обществени компютри, като тези в хотелите или интернет кафенетата, за да влизате в акаунтите си. Тъй като всеки може да използва тези компютри, те могат да са заразени и да запаметят всички ваши удари по клавиатурата. Влизайте в акаунтите си само от доверени компютри или мобилни устройства.
4. Бъдете внимателни, когато уебсайтове изискват да отговаряте на лични въпроси. Тези въпроси се използват при забравяне на фразата ви за достъп и нужда от нулирането ѝ. Проблемът е, че отговорите на тези въпроси могат често да бъдат намерени в интернет или дори на Facebook страницата ви. Когато отговаряте на лични въпроси, старайте се да давате само информация, която не е обществено достъпна или е измислена информация, която сте

Фрази за достъп

си съчинили. Не можете да запомните всички отговори на въпросите си за сигурност? Изберете тема, като филмов герой например, и основавайте отговорите си на този герой. Друга опция е, ако използвате софтуер за управление на пароли - повечето от тези програми ви позволяват да съхранявате и тази допълнителна информация.

5. Много онлайн акаунти предлагат нещо, което се нарича оторизация от два фактора, или проверка от две стъпки. Това е при случаите при които са ви наобходими повече от една фраза за достъп, като например парола, която се изпраща на мобилния ви телефон. Тази опция е много по-сигурна, отколкото само една фраза за достъп. Когато е възможно, винаги активирайте и използвайте тези по-сигурни начини за проверка.
6. Мобилните устройства често изискват PIN код, който да защитава достъпа до тях. Помнете, че PIN кодът не е нищо повече от още една парола. Колкото по-дълъг е PIN кодът ви, толкова по-сигурен е. Много мобилни устройства ви позволяват да промените PIN номера си на реална фраза за достъп или да използвате биометрична подкрепа, като отпечатък от пръста ви.
7. Ако вече не използвате акаунт, уверете се, че той е затворен, изтрит или деактивиран.

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

Управление на пароли:	https://securingthehuman.sans.org/ouch/2015#october2015
Оторизация от две стъпки:	https://securingthehuman.sans.org/ouch/2015#september2015
Заключване на информация за влизане в офиса:	https://lockdownyourlogin.com
SANS SEC301 – Петдневен курс за основите на кибер сигурността:	https://sans.org/sec301

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

