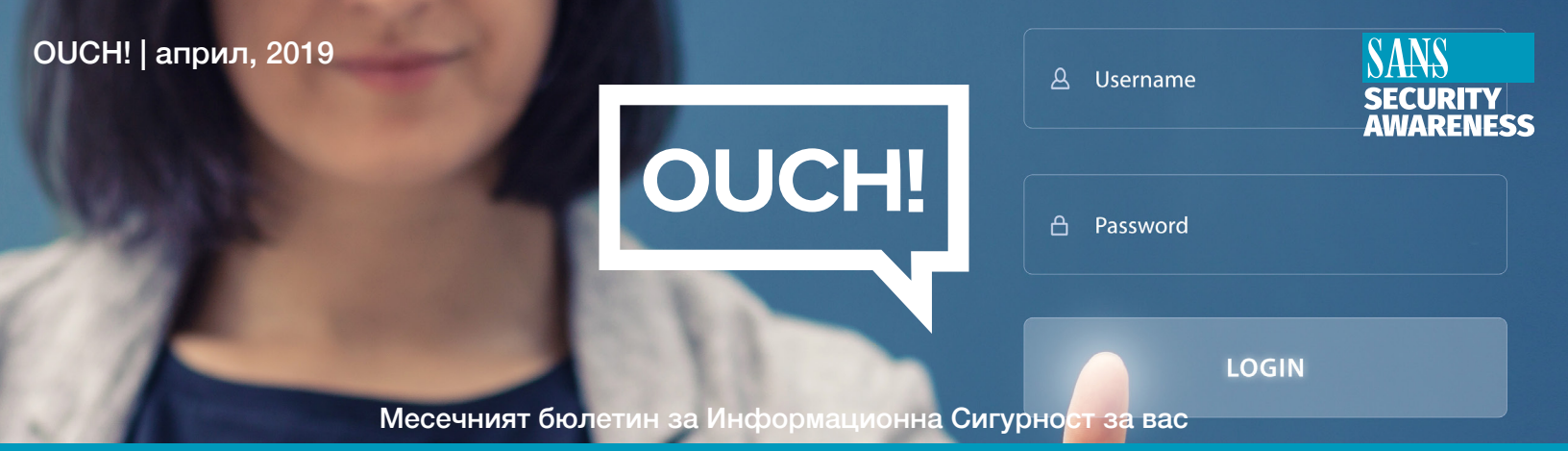

Месечният бюлетин за Информационна Сигурност за вас

Да направим паролите лесни

Преглед

Често ни се казва, че паролите ни са ключът към защитата на акаунтите ни (което е вярно!), но рядко се препоръчва лесен начин да създаваме и управляваме всичките тези пароли. По-долу ще застъпим три прости стъпки, с които да опростите паролите си, заключите акаунтите си и защитите бъдещето си.

Фрази-пароли

Дните на безумно сложните пароли са в миналото. Тези пароли са трудни за запомняне, трудни за писане, и със съвременните супер бързи компютри са лесна плячка за кибер престъпниците. Ключът към добрите пароли е да са дълги - колкото повече символи, толкова по-добре. Наричат се фрази-пароли и представляват вид силна парола от кратко изречение или случайни думи. Ето два примера:

Vreme za edno silno kafe!
izguben-ohluv-pylzi-plaj

И двете са силни, съставени от повече от 20 символа, лесни за запомняне и писане, но трудни за хакване. Има ситуации и уебсайтове изискващи символи, цифри или главни букви, което не е проблем. Винаги помнете, че дължината е най-важна.

Мениджъри за пароли

Нужна ви е уникална парола за всеки акаунт. Ако използвате една и съща парола за множество акаунти, поемате сериозен риск. Всичко, което кибер престъпниците трябва да направят, е да хакнат един от сайтовете, който ползвате, откраднайки всички пароли, включително вашата, и после да използват паролата за достъп до другите ви акаунти. Случва се доста по-често, отколкото може би осъзнавате. Не вярвате? Погледнете уебсайта www.haveibeenpwned.com, за да видите кои сайтове, които ползвате, са били хакнати и евентуално паролата ви за тях е била компрометирана. Какво би могло да се направи? Използвайте мениджър за пароли.

Това са специални компютърни програми, които пазят на сигурно място всичките ви пароли в криптиран виртуален сейф. Нужно е да помните само една парола, тази за мениджъра ви за пароли. Тези програми автоматично извличат паролите ви, когато са ви нужни, и ги предоставят на уебсайта вместо вас. Те имат и други полезни функции, като

например съхраняване на отговорите на тайни въпроси, предупреждаване когато използвате парола повече от веднъж, генератори на пароли, които да ползвате за силни пароли, и много други. Повечето мениджъри за пароли се синхронизират между различни устройства, така че да имате лесен и сигурен достъп до всичките си пароли независимо от това коя система ползвате.

Накрая, уверете се че сте си записали паролата си за мениджъра за пароли и сте я съхранили на сигурно място у дома. Някои мениджъри за пароли дори предоставят за разпечатване комплект за възстановяване на изгубен достъп. По този начин, дори ако забравите паролата си за мениджъра на пароли, имате резервен вариант. Това също е полезно при спешни случаи, когато някой трябва да получи достъп вместо вас.

Двустепенно удостоверявне

Удостоверяването в две стъпки (често наричано Two-factor Authentication или Multi-factor Authentication) добавя допълнително ниво на защита. То изисква от вас да разполагате с 2 елемента за достъп до акаунтите ви – парола и цифров код, обикновено генериран от смартфона ви или изпратен като съобщение. Този процес гарантира, че дори кибер престъпници да се сдобият с паролата ви, това няма да им даде достъп. Удостоверяването в две стъпки е просто за настройване и обикновено има нужда да го ползвате само веднъж, ако се логвате от ново устройство или компютър. Включете го, където е налично, особено за най-важните ви акаунти, като например банкови и пенсионни сметки, или достъпа до имейла ви. Ако използвате мениджър за пароли, горещо ви препоръчваме да го защитите със силна парола И удостоверяване в две стъпки.

Може да звучи странно, но тези три прости стъпки имат огромна полза за опазването на вашата работа и репутация, както и на финансовото ви бъдеще.

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

Гост-редактор

Джъстин Хендерсън *(@SecurityMapper) е съосновател на H & A Security Solutions, сертифициран SANS Institute инструктор и автор на SANS курсове за кибер защита и SIEM. Той обича всичко свързано с кибер защита и се занимава с консултиране от 15 години.*

Ресурси

Have I Been Pwned:	https://haveibeenpwned.com/
Удостоверяване в две стъпки:	https://twofactorauth.org/
NIST SP800-63B Digital Identity Guidelines:	https://pages.nist.gov/800-63-3/sp800-63b.html
Poster: You Are a Target:	https://www.sans.org/u/OGi