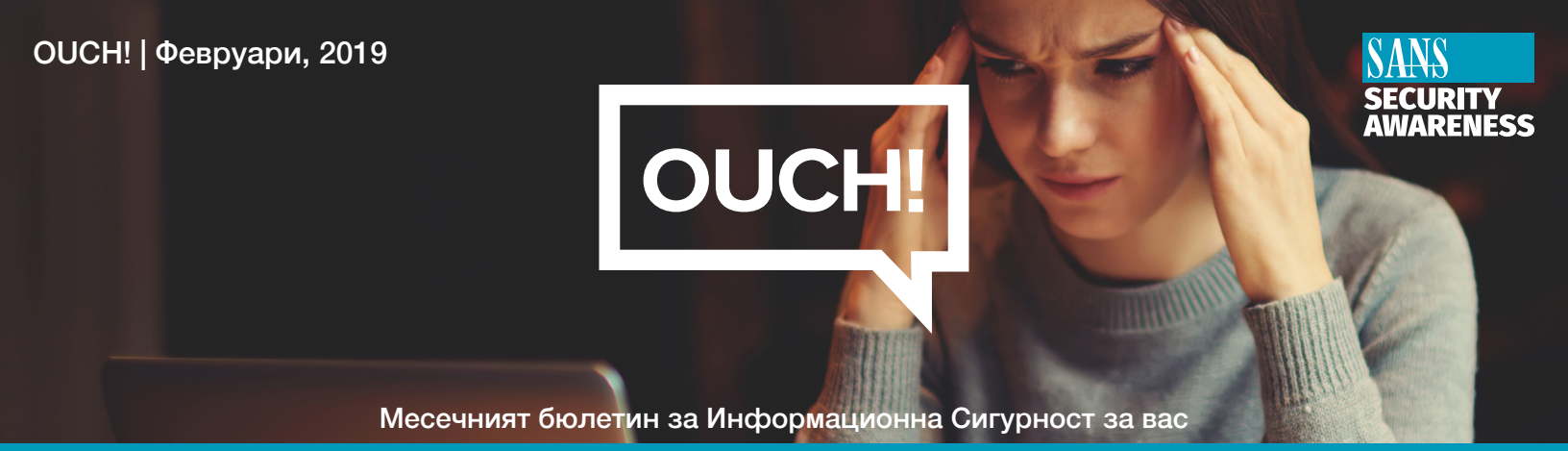
OUCH! | Февруари, 2019



Месечният бюлетин за Информационна Сигурност за вас

Персонализирани измами

Преглед

Кибер престъпниците продължават да измислят нови начини да измамят хората. Нов вид измама набира популярност – персонализирани измами. Кибер престъпниците намират или купуват информация за милиони хора, след което използват тази информация за да персонализират атаката си. По-долу ще покажем как работят тези измами заедно с често срещани примери. Колкото повече знаете за тях, толкова по-лесно е да ги забележите и спрете.

Как работи?

Измамите по телефон или имейл не са новост, кибер престъпниците от години се опитват да мамят хора с тях. Примерите включват „Печалба от лотарията“ или добре известната измама „Нигерийски принц“. В тези традиционни измами кибер престъпниците не знаят кого всъщност атакуват. Те просто създават обикновено съобщение и го пращат на милиони хора. Тъй като тези измами са повтарящи се, те са обикновено се забелязват лесно. Персонализираните измами са различни, кибер престъпниците първо проучват жертвата си и създават персонализирано съобщение за всяка една потенциална жертва. Това се случва чрез намиране или купуване на база данни с имена, пароли, телефонни номера или други данни. Този вид информация е лесно достъпен заради всички уебсайтове, които са били хакнати. Също така често тази информация е достъпна чрез социалните мрежи или публикувани правителствени документи. Престъпниците атакуват всеки, за когото имат информация.

Често срещан трик използван от кибер престъпниците е страх или изнудване за да ви накарат да платите. Ето как работи атаката. Те намират или купуват информация за потребителски имена и пароли от хакнати уебсайтове. Използвайки тази информация, те изпращат както на вас така и на всеки друг в базата данни имейл със лична информация за получателя, включително паролата, която е ползвана за уебсайта. Престъпниците наричат паролата ви „доказателство“ за това, че са хакнали компютъра или устройството ви, което разбира се не е вярно. Престъпниците след това твърдят, че докато са хаквали компютъра ви, са ви хванали да гледате порнография онлайн. Следва заплаха, че ако не платите откуп, неудобни доказателства за вашите онлайн „дейности“ ще бъдат споделени със семейството и приятелите ви.

Уловката е в това, че в почти всички случаи кибер престъпниците изобщо не са хаквали системата ви. Те не знаят кой сте, нито кои уебсайтове сте посещавали. Те просто се опитват да използват няколко лични детайла които имат за да

ви изплашат и да ви накарат да повярвате, че са хакнали компютъра или устройството ви, и да ви убедят да им платите. Не забравяйте, че същият метод може да се използва и за телефонна измама.

Какво да направя?

Научете се да разпознавате такива обаждания или имейли като измами. Нормално е да се уплашите от това, че някой има ваши лични данни. Помнете – изпращачът лъже. Атаката е част от автоматизирано масово изпращане на имейли, а не опит да атакуват директно вас. В днешно време е много по-лесно за кибер престъпниците да намерят или купят лични данни, така че очаквайте повече такива персонализирани измами да се случват в бъдеще. Ето няколко улики, за които да внимавате:

- **Винаги когато получите много спешен имейл, съобщение или телефонно обаждане, бъдете нащрек. Ако някой използва емоции като страх или спешност, значи се опитват да ви накарат да направите грешка от припряност;**
- **Ако някой иска заплащане в BitCoin, ваучери или други непроследими методи;**
- **Ако получите подозрителен имейл, потърсете с Гугъл да проверите дали други хора не са споделили за нещо подобно.**

Здравият разум е най-добрата защита. Препоръчваме ви да използвате уникална, дълга парола за всеки отделен онлайн акаунт. Не можете да помните толкова пароли? Използвайте мениджър на пароли. В допълнение, използвайте удостоверяване в две стъпки където е възможно.

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

Лени Зелцер *е ветеран в киберсигурността. Той работи по създаването на антивирусни решения в Minerva Labs и преподава класове по сигурност в SANS Institute. Опитът му също включва услуги и консултации в сигурността. Последвайте го на* zeltser.com/blog *или в Туитър на* @lennyzeltser.

Ресурси

Социално инженерство:	https://www.sans.org/u/MUU
Спрете този фишинг:	https://www.sans.org/u/MUZ
Потърсете се онлайн:	https://www.sans.org/u/MV4
Мениджъри на пароли:	https://www.sans.org/u/MV9