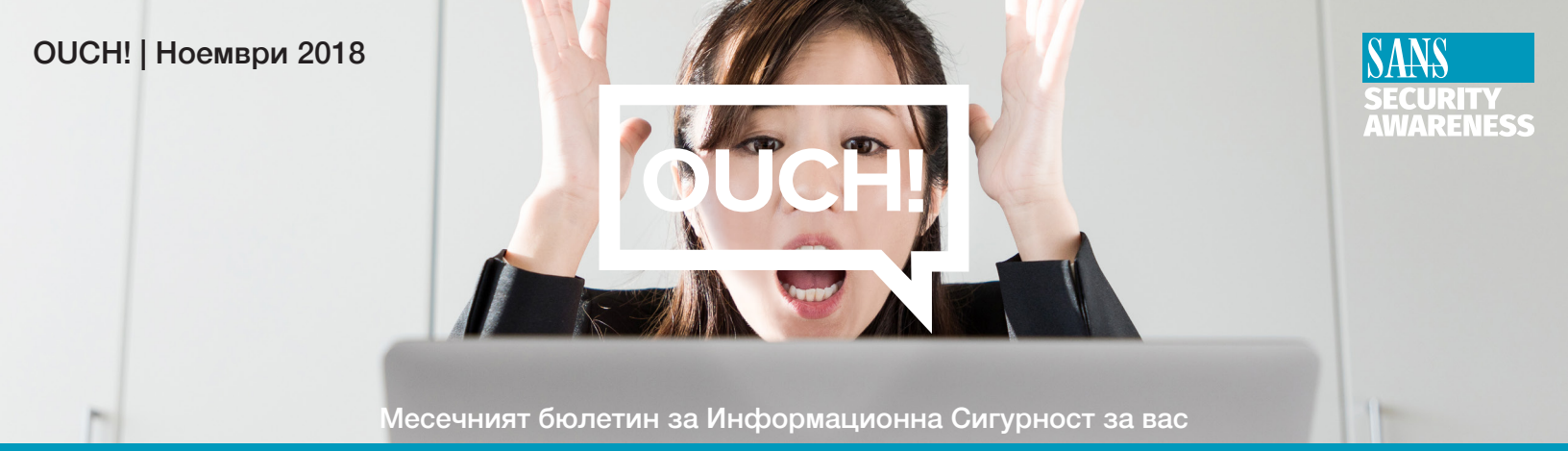

Месечният бюлетин за Информационна Сигурност за вас

Хакнали ли са ме?

Преглед

Без значение колко сте уверени в собствената си сигурност, точно както при шофирането, рано или късно ще попаднете в инцидент. Тук сме представили няколко идеи, които ще помогнат да разберете дали сте станали жертва на хакери, и ако е така, какво да направите. Колкото по-скоро разберете, че нещо се е случило, толкова по-вероятно е да се справите с проблема.

Знаци, че сте жертва на хакери

Антивирусната ви програма съобщава, че системата ви е заразена. Уверете се, че подобни съобщения идват от антивирусния софтуер, а не от изскачащ прозорец на уеб сайт, опитващ се да ви подмами да се обадите някъде или да инсталирате нещо друго. Не сте сигурни? Погледнете антивирусната си програма.

Виждате надпис, че компютърът ви е криптиран и трябва да платите откуп, за да си получите файловете обратно.

Уеб браузърът ви показва всякакъв вид сайтове, които не сте отваряли.

Компютърът или приложенията ви постоянно се сриват, появяват се странни нови икони, приложения или прозорци.

Паролата ви не работи, а сте сигурни, че въвеждате правилната такава.

Приятели ви питат защо им пращате странни съобщения по имейл, които сте сигурни, че никога не сте пращали

Имате разходи по кредитна карта или тегления от банковата ви сметка, които не са направени от вас.

Как да реагирате

Ако смятате, че сте жертва на хакери, колкото по-бързо действате, толкова по-добре. Ако е свързано с работата ви, не се опитвайте да отстраните сами проблема, а докладвайте незабавно. Ако става въпрос за личната ви система или акаунт, ето няколко стъпки, които можете да предприемете

Сменете паролите си: Това включва не само смяна на паролите на компютрите и мобилните ви устройства, но и на онлайн акаунтите ви. Не използвайте хакнатия компютър за смяната на паролите, използвайте различна система, за която сте уверен, че е сигурна. Ако имате много акаунти, започнете с най-важните. Невъзможно е да се следят всички акаунти, затова използвайте мениджър за пароли.

Финанси: За проблеми с кредитни карти или всякакви финансови сметки, обадете се веднага на банката или издателя на картата. Използвайте доверен телефонен номер за обаждането, например такъв който е написан на гърба на картата ви, на извлечение или на официалния уеб сайт, посетен от сигурен компютър. Обмислете дали да не сложите забрана за теглене на кредити от ваше име.

Антивирус: Ако антивирусната ви програма съобщава за заразен файл, следвайте препоръчаните от нея инструкции. Повечето антивирусни програми предоставят връзки, на които можете да откриете повече информация за конкретния вирус.

Преинсталиране: Ако не можете да се справите с инфектиран компютър, или искате да сте сигурни, че системата ви е безопасна, преинсталирайте операционната система. Не преинсталирайте от резервни копия, те трябва да се използват само за възстановяване на личните ви файлове. Ако не се чувствате комфортно с това, обмислете дали да не използвате професионална услуга. В някой случаи, ако устройството е старо, може да е по-лесно директно да се купи ново. Накрая, след като системата ви е възстановена или имате нова такава, убедете се, че е обновена и че автоматичното обновяване е включено, където е възможно.

Архиви: Ключов момент за да сте подготвени е да имате достатъчно скорошен архив. Много продукти архивират автоматично данните ви дневно, или дори ежечасно. Без значение какво ползвате, винаги проверявайте дали можете да възстановявате файловете си. Доста често възстановяване от архив е единствения начин да си върнете данните, след като сте били жертва на хакери.

Полиция: Ако се почувствате застрашени по някакъв начин, докладвайте в местната полиция. Ако сте жертва на кражба на идентичност и живеете в САЩ, посетете https://www.identitytheft.gov.

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

Д-р Йоханес Улрих *(@johullrich) е декан на научно-изследователската дейност в SANS Technology Institute, директор на SANS Internet Storm Center и сътрудник на SANS. Той е създателят на DShield – мрежа за взаимопомощ, и автор на ежедневния подкаст на Internet Storm Center за мрежова информационна сигурност.*

Ресурси

Архиви:	https://www.sans.org/u/JGP
Фрази-пароли:	https://www.sans.org/u/JGU
Мениджъри за пароли:	https://www.sans.org/u/JGZ
Какво са вирусите:	https://www.sans.org/u/JH4
Централен Кредитен Регистър:	http://www.bnb.bg/AboutUs/AUFAQ/CONTR_CREDIT_REGISTER_FAQ

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