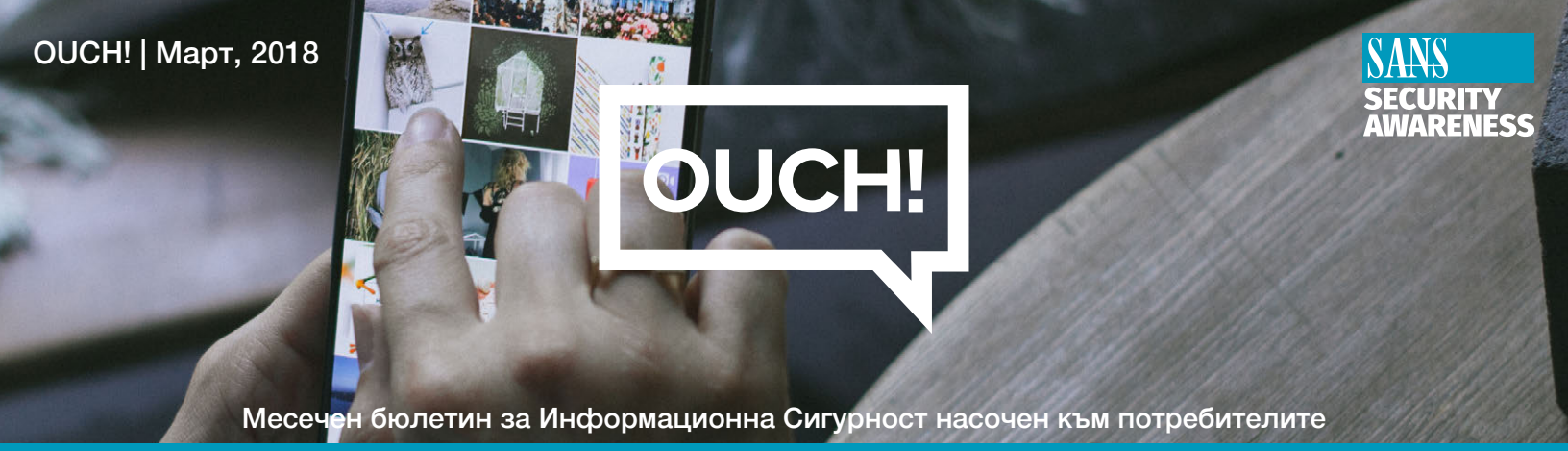

Месечен бюлетин за Информационна Сигурност насочен към потребителите

Топ съвети за сигурно ползване на социални медии

Преглед

Социалните медии като Snapchat, Facebook, Twitter, Instagram и LinkedIn са чудесни ресурси, позволяващи ви да срещнете, комуникирате и споделяте с хора от целия свят. С това обаче идват и рискове – не само за вас, но и за семейството ви, приятелите ви и работодателя ви. В този бюлетин предоставяме ключовите стъпки към пълноценното използване на социалните медии сигурно и безопасно.

Публикуване

Бъдете внимателни и мислете, преди да публикувате. Всичко, което публикувате, най-вероятно ще бъде публично достъпно в даден момент, повлиявайки на на репутацията ви и бъдещето ви, включително на това в кое училище ще бъдете приети и кои работни места ще получите. Ако не искате семейството или шефът ви да видят нещо, най-добре е да не го публикувате. Също така бъдете наясно какво другите публикуват относно вас самите. Може да се наложи да поискате от някого да премахне нещо, свързано с вас.

Поверителност

Почти всички социални медии имат отлични опции за поверителност – използвайте ги, където е възможно. Например, наистина ли този сайт има нужда да проследява къде се намирате? В допълнение, опциите за поверителност могат да са объркващи, и често да бъдат променяни. Създайте си навик да проверявате дали работят така, както очаквате.

Фрази за достъп

Подсигурете акаунта си с дълга и сигурна фраза за достъп. Фразата за достъп е парола, съставена от много думи, правеща я лесна за въвеждане и запомняне от вас, но трудна за кибер престъпниците да отгатнат.

Заключете акаунта си

Още по-добре бихте направили, ако включите удостоверяването в две стъпки за всичките си акаунти. Това добавя изискване за еднократен код в добавка към паролата ви, когато искате да влезете в акаунта си. Това всъщност е доста лесно и е един от най-мощните начини да защитите акаунта си.

Измами

Точно както при електронната поща, злосторниците ще се опитат да ви подмамят или излъжат в социалните медии. Например, биха могли да се опитат да ви убедят да им дадете паролата си или номер на кредитна карта.

Внимавайте на какво кликвате: ако приятел ви изпрати странно съобщение, или не звучи като да е този човек, възможно е да е кибер престъпник, който се преструва на приятеля ви.

Условия за ползване

Запознайте се с условията за ползване на услугата. Всяко нещо, което публикувате или качвате може да стане собственост на сайта.

Работа

Ако искате да публикувате нещо, свързано с работата ви, допитайте се първо до прекия си началник, за да сте сигурни, че това е допустимо.

Следвайте тези съвети, за да се радвате на много по-сигурно онлайн преживяване. За да научите повече за това как да ползвате социални медии безопасно или да докладвате за нещо съмнително, обърнете се към уеб страницата по сигурността на съответната социална медия.

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

Джесика Баркър е световен лидер в човешкия фактор на кибер сигурността. Тя е съосновател на Redacted Firm, където предоставя консултантски услуги на клиенти по целия свят, и е известен говорител. Последвайте я в Туитър на @drjessicabarker.

Ресурси

Фрази за достъп:	https://www.sans.org/u/B6E
Удостоверяване в две стъпки:	https://www.sans.org/u/B6J
Онлайн сигурност за децата:	https://www.sans.org/u/B6O
Заключете входа:	https://www.lockdownyourlogin.org/

lisensi