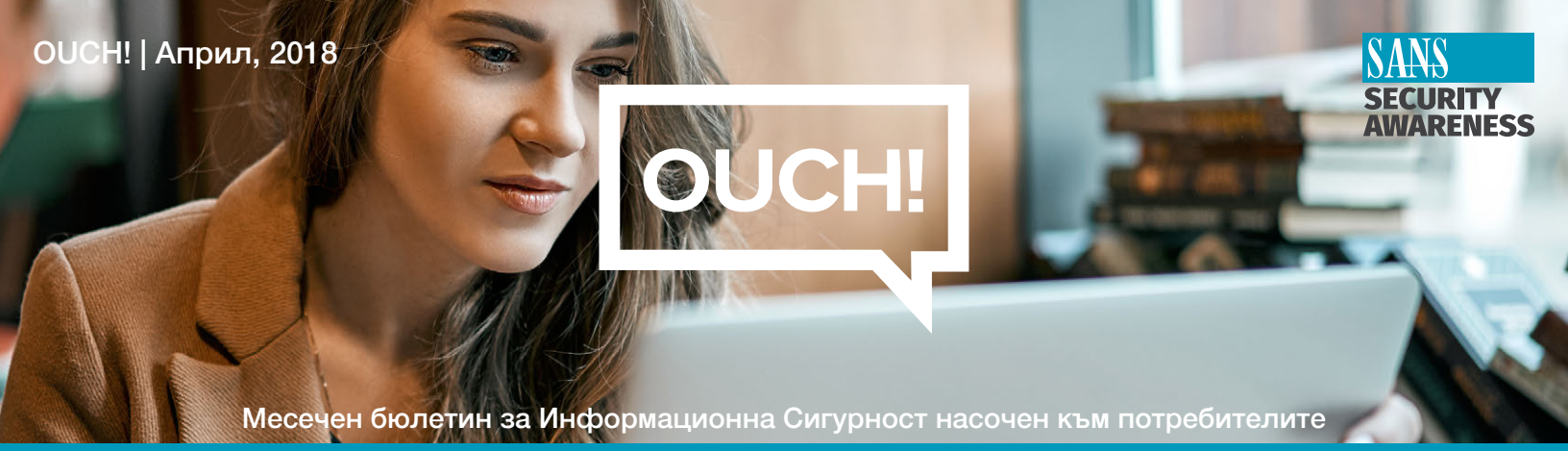

Месечен бюлетин за Информационна Сигурност насочен към потребителите

Спрете този фишинг

Преглед

Услугите за електронна поща и съобщения (като Skype, Twitter или Snapchat) са един от основните начини за комуникация. Използваме тези технологии не само всеки ден за работа, но и да поддържаме връзка с приятелите и семейството си. Тъй като толкова много хора по света зависят от тези технологии, те са се превърнали в един от основните начини за атакуване, използвани от киберпрестъпници - метод на атака, наречен фишинг. Научете какво е фишинг и как можете да забележите и спрете тези атаки, независимо дали сте на работа или у дома.

Какво е фишинг

Фишингът е тип атака, която използва имейл или услуга за изпращане на съобщения, за да ви заблуди да предприемете действие, което иначе не бихте направили, като кликване върху злонамерена връзка, споделяне на паролата ви или отваряне на заразен файл прикачен към имейл. Атакуващите работят усилено, за да направят тези послания убедителни и да отключат емоционална мотивация, като създават например чувство за спешност или любопитство. Те могат да ги накарат да изглеждат така, сякаш идват от някой или нещо, което познавате, като приятел или доверена компания, която често използвате. Могат дори да добавят логото на вашата банка или да фалшифицират имейл адреса на подателя, така че съобщението да изглежда по-легитимно. Атакуващите изпращат тези съобщения на милиони хора. Те не знаят кой ще клъвне; всичко, което знаят е, че колкото повече изпращат, толкова повече хора ще се хванат.

Защитете се

В почти всички случаи, отварянето и четенето на имейл или съобщение не е проблем. За да проработи фишинг атаката, трябва да ви подмамят да направите нещо. За щастие има знаци, че посланието е атака, ето тук са най-често срещаните:

- Силно усещане за спешност, което настоява за незабавни действия, преди да се случи нещо лошо, като заплашва да закрие сметката ви или да ви изпрати в затвора. Атакуващият иска да ви притисне да направите грешка.
- Натиск да заобиколите или игнорирате правила или процедури на работното място.
- Силно усещане за любопитство или предлагане на нещо прекалено добро, за да е истина (не, не сте спечелили от лотарията).

- Общ поздрав като „Уважаеми клиенти“. Повечето компании или приятели, които се свързват с вас, знаят името ви.
- Искане за изключително чувствителна информация, като например номера на кредитната ви карта или паролата ви или всяка друга информация, която истинският изпращач трябва да знае.
- Съобщението твърди, че идва от официална организация, но има лоша граматика или правопис или използва личен имейл адрес като @gmail.com.
- Съобщението идва от официален имейл (като например шефа ви), но има различен адрес за отговор.
- Получавате съобщение от някой, когото познавате, но тонът или формулировката просто не звучат като него или нея. Ако подозирате проблем, обадете се на изпращача, за да потвърдите, че той го е изпратил. За кибер атакуващия е лесно да създаде съобщение, което изглежда да е от приятел или колега.

В крайна сметка здравият разум е вашата най-добра защита. Ако имейл или съобщение изглежда странно, подозрително или твърде добро, за да е истина, може да е фишинг атака.

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

Тоня Дъдли (Tonia Dudley) разработва и ръководи програми за сигурност от 2011 г., което включва изграждането на програма за обучение по фишинг, която е носител на награди. Можете да я намерите на - www.linkedin.com/in/toniadudley.

Ресурси

Социално инженерство:	https://www.sans.org/u/Cb1
Помогнете на другите:	https://www.sans.org/u/Cb6
Имейли – какво да правим и да не правим:	https://www.sans.org/u/Cbg
Измамите на фалшивия шеф:	https://www.sans.org/u/Cbl
Ouch! Преводи и архиви:	https://www.sans.org/u/Cbq

lisensi

OUCH! се публикува от SANS Securing The Human и се разпространява под лиценза на Creative Commons BY-NC-ND 4.0. Имате право да разпространявате този бюлетин или да го използвате във вашата информационна кампания, при условие че не го модифицирате. За преводи или повече информация моля пишете на www.sans.org/security-awareness/ouch-newsletter. Редакторски колектив: Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли | Превод: Николай Дачев и Радослава Несторова