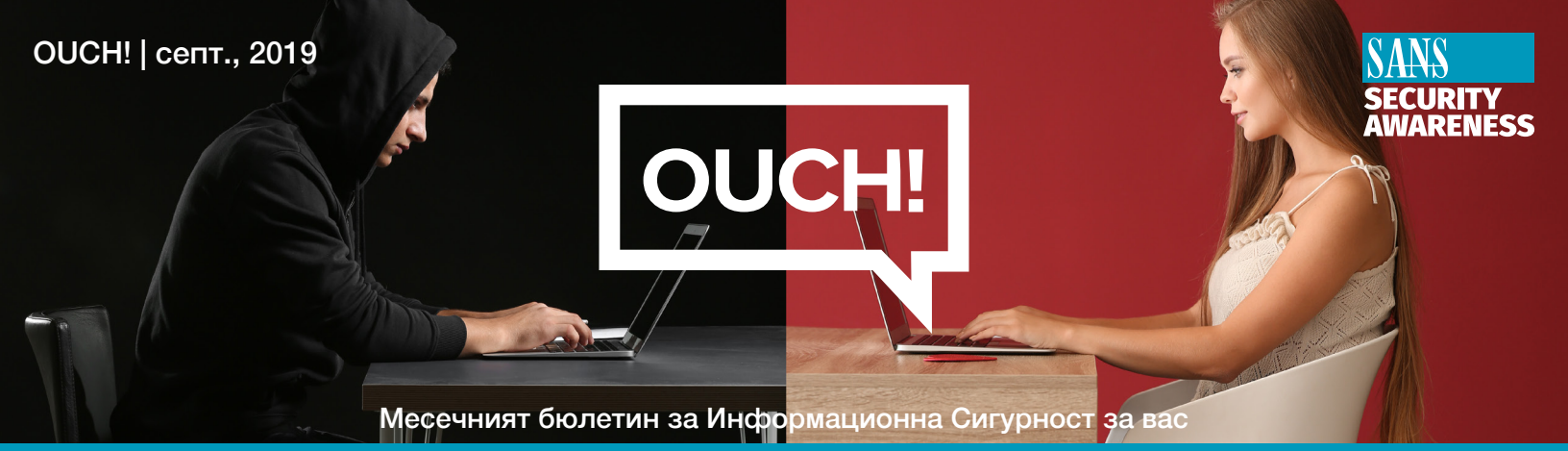
OUCH! | септ., 2019



Месечният бюлетин за Информационна Сигурност за вас

Измама чрез социалните медии

Преглед

Много от нас са получавали фишинг атаки по имейл, както на работа, така и у дома. Това са имейли, които изглеждат легитимно, например от вашата банка, от шефа ви или от любимия ви онлайн магазин. Всъщност обаче те са атака, която се опитва да измами или да ви накара прибързано да предприемете действие, което не трябва да предприемате, като например да отворите заразен прикачен файл, да споделите паролата си или да преведете пари. Предизвикателството е, че колкото по-интелигентни ставаме в забелязването и спирането на тези имейл атаки, толкова повече кибер престъпниците изпробват други начини за контакт и измама на хората.

Опитите за измама или залъгване могат да се случат в почти всяка форма на комуникация, която използвате, от Skype, WhatsApp и Slack до Twitter, Facebook, Snapchat, Instagram или дори приложения за игри. Комуникацията през тези платформи или канали може да се усеща по-неформална или достоверна, и именно затова атакуващите ги използват, за да заблудят другите. В допълнение, с днешните технологии е вече много по-лесно всеки атакуващ навсякъде по света да се преструва на какъвто и да е, или на когото пожелае. Важно е да запомните, че всяка комуникация, която осъществявате, може да не е такава, каквато изглежда, и че хората не винаги са такива за каквито се представят.

Ключови бележки

Ето най-често срещаните улики, че съобщението, което току-що сте получили, или публикацията, която току-що сте прочели, може да бъде атака.

Спешност: Съобщение, което има чувство за неотложност, което изисква „незабавни действия“ преди да се случи нещо лошо, като заплаха да ви закрият акаунт или да ви изпратят в затвора. Атакуващият иска да ви накара да избързате и да направите грешка.

Натиск: Притискат ви да заобиколите или игнорирате политики или процедури на работа.

Любопитство: Силно чувство на любопитство или нещо, което е твърде добро, за да е истина. Не, не сте спечелили от лотарията.

Поверителност: Искане за силно поверителна информация, като номер на вашата кредитна карта или парола, или всяка информация, която просто не се чувствате удобно да споделяте.

Официални съобщения: В съобщението се казва, че идва от официална организация, но има грешна граматика или правопис. Повечето правителствени организации няма да използват социалните медии за официална комуникация директно с вас. Ако не сте сигурни дали съобщението е легитимно, обадете се на организацията, но използвайте доверен телефонен номер, например такъв от уебсайта им.

Представяне за друг: Получавате съобщение от приятел или колега, но тонът или формулировката просто не звучат като този човек. Ако заподозрете, обадете се на подателя по телефона, за да проверите дали той наистина е изпратил съобщението. За кибер атакуващия е лесно да създава съобщения, които изглеждат като да са от някой, когото познавате. В някои случаи те могат да откраднат акаунта на вашия приятел, след което да се преструват на него и да се свържат с вас. Бъдете особено нащрек с текстови съобщения, Twitter и други формати на кратки съобщения, при които е по-трудно да разберете личността на изпращача.

Вие сте най-добрата защита срещу подобни измами, лъжливи съобщения и атаки. Ако публикация или съобщение ви изглежда странно или подозрително, просто го игнорирайте или го изтрийте, или ако е от някой, когото познавате лично, обадете се на човека по телефона, за да потвърди дали наистина го е изпратил.

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 Джесика Баркер *(@drjessicabarker) е лидер в човешката страна на кибер сигурността. Тя е съ-изпълнителен директор на Cygenta, където следва страстта си да влияе положително върху информираността, поведението и културата в кибер сигурността по целия свят. Тя е председател на ClubCISO и популярен водещ лектор.*

Ресурси

Социално инженерство:	https://www.sans.org/u/Uz6
Измами с телефонни обаждания:	https://www.sans.org/u/Uzb
Спрете с фишинга:	https://www.sans.org/u/Uzg
Персонализирани измами:	https://www.sans.org/u/Uzl