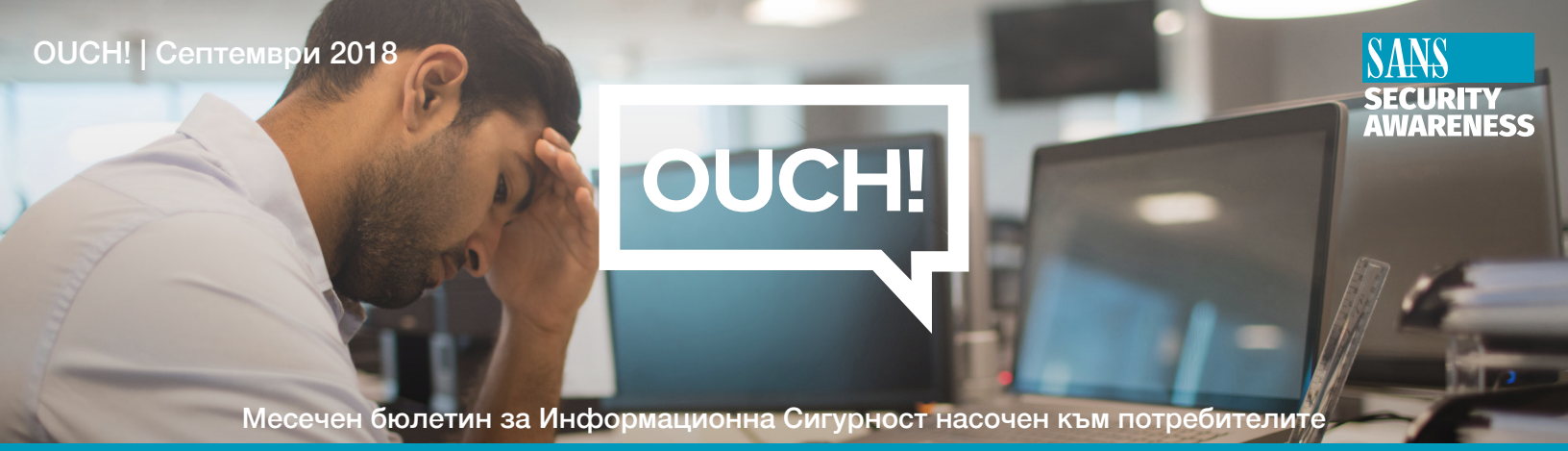

Месечен бюлетин за Информационна Сигурност насочен към потребителите

Компрометиран бизнес имейл

Какво е измамата „Изпълнителен Директор“ и компрометиран бизнес имейл?

Кибер престъпниците непрекъснато усъвършенстват вид имейл атака наречена „Измама Изпълнителен Директор“ (CEO Fraud), или компрометиран бизнес имейл (BEC). Това са насочени атаки, целящи да подмамят жертвата да предприемат действие, което иначе не биха направили. В повечето случаи лошите целят финансова изгода. Тези атаки са толкова опасни, тъй като атакуващия проучва жертвата си, преди да предприеме действия. Също така е много трудно тези атаки да бъдат спрени с технологични средства, тъй като няма инфектиран прикачен файл или връзка, които да бъдат засечени.Ето как работи атаката.

Кибер престъпника използва Интернет, за да проучи жертвата си, както и хора, с които тя е свързана. Например, ако изберат вас, биха проучили кой е началникът ви на работа, или пък подробности за работата ви (например – надомен брокер недвижими имоти). След това престъпниците създават имейл, в който се представят за някой от хората, с които работите, и ви го изпращат. Имейлът е спешен, изисква незабавна реакция, като например да се обработи фактура, промяна на получател на плащане, или пък с искане за важни документи. Имейлът цели да ви притисне по начин, който да ви накара да направите това, което се иска. Ето два примера за това как би проработила подобна атака:

Банков Превод: Престълникът търси директна парична печалба. Той проучва компанията, за която работите, откривайки например кой е оперативния счетоводител, или който и да е служител отговорен за парични преводи. След това се създава и изпраща имейл до тези служители, преструвайки се на началника им или друг висшестоящ служител. Имейлът им съобщава, че има спешен случай, и трябва незабавно да се преведат пари на нова банкова сметка. Имейлът ги притиска така, че да допуснат грешка, и те всъщност изпращат парите на престъпника.

Данъчни измами: Престъпниците търсят лични данни на хора с цел данъчни измами. Един от най-бързите начини за това е да се открадне информацията на всички служители в една компания. Престъпниците проучват и идентифицират кой работи в „Човешки Ресурси“. След това те изпращат фалшив имейл, преструвайки се на висшестоящ служител или юрисконсулт. Имейлът представя измислена история, според която личните данни за всички служители трябва да бъде незабавно предоставена. Служителите в „Човешки ресурси“ смятат, че изпращат тази поверителна информация на колега, докато всъщност я предоставят на кибер престъпниците.

Как да се защитим

Какво можем да направим, за да се защитим? Здравият разум е най-добрата защита. Ето най-честите улики, за които да следим:

- **Имейлът е много кратък и спешен (често само няколко изречения), и според подписът е изпратен от мобилно устройство.**
- **Има силно усещане за спешност, притискайки ви да игнорирате или заобиколите политиката на компанията. Винаги следвайте политиката и процедурите на компанията, дори и искането да е от прекия ви началник или самият Изпълнителен директор.**
- **Имейлът е свързан с работата, но използва личен адрес, например @gmail.com или @hotmail.com.**
- **Имейлът изглежда така, сякаш идва от висшестоящ, колега или доставчик с когото работите или познавате, но тонът на съобщението не е типичен за тях.**
- **Предоставени са инструкции за плащане, които са различни от тези, с които разполагате, например искане за незабавно плащане към различна банкова сметка.**

Ако подозирате, че сте атакуван в работата, спрете всякакво взаимодействие и докладвайте лично на прекия си началник. Ако сте атакуван у дома, или вече е извършен паричен трансфер, незабавно уведомете банката си, след което съобщете в полицията.

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

Дон Кавендър *е бивш ФБР специален агент, заминавал се повече от 22 години с компютърни разследвания и кибер престъпност. Последното му начинание е като координатор по компрометиране на бизнес имейл във Вашингтон и е насочено срещу организирани престъпни групи. Той също така предоставя обучение и проучвания в компютърните и кибер разследвания.* @don_cavender https://www.linkedin.com/in/donald-cavender

Ресурси

Социално инженерство:	https://www.sans.org/u/HE3
Спрете този фишинг:	https://www.sans.org/u/HE8
Спрете тези вируси:	https://www.sans.org/u/HEd
Заключете достъпа:	https://www.sans.org/u/HEi

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