Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- Какво е CEO Fraud (Измама Изпълнителен директор)?
- Как да се предпазим

Измама Изпълнителен Директор

Какво е CEO Fraud (Измама Изпълнителен директор)?

Кибер престъпниците са подли - постоянно измислят нови начини да получат това, което искат. Един от най-ефективните методи е да се насочат към хора като вас. Кибер нападателите са се научили, че незнаещите хора са най-слабото звено във всяка организация, но са забравили, че знаещите хора като читателите на OUCH! могат да бъдат най-добрата защита на една организация.

Гост-редактор

Анжела Папас е директор на отдела по обучение и информираност по информационна сигурност на Thomson Reuters. В своята работа, Анжела отговаря за посланическата програма, електронното обучение и обучението на служителите за фишинг.

Кибер престъпниците са разработили нова атака наречена CEO Fraud (Измама Изпълнителен директор, известна също като Business Email Compromise (BEC) /Компрометиране на бизнес имейл/. В тези атаки, кибер престъпникът се представя за главен изпълнителен директор или друг висш служител от вашата организация. Престъпникът изпраща съобщение до служителите като вас и се опитва да ви подведе да направите нещо, което не трябва да правите. Тези видове атаки са изключително ефективни, тъй като кибер престъпниците правят проучване. Те намират уебсайта на организацията ви и търсят информация, като например къде се намира, кои са вашите мениджъри и други организации, с които работите. След това кибер престъпниците научават всичко възможно, за колегите ви в сайтове като LinkedIn, Facebook или Twitter. След като узнаят структурата на организацията ви, те започват да проучват и да се насочват към определени служители. Избират мишените си въз основа на специфичните си цели. Ако кибер престъпниците търсят пари, могат да се насочат към служители в отдела по плащане на сметки. Ако търсят данъчна информация, могат да се насочат към човешки ресурси. Ако искат достъп до сървърите с бази данни, биха могли да се насочат към някой в IT отдела.

След като определят какво искат и в кого ще се целят, те започват изработването на атаката си. Най-често използват spear phishing (насочен фишинг). Фишинг е, когато атакуващият изпраща имейл до милиони хора, с цел да ги излъже да направят нещо, например отваряне на заразен прикачен файл или посещение на злонамерен сайт. Spear phishing е подобен на фишинга, но вместо да се изпраща общ имейл на милиони хора, те изпращат персонализирани имейл насочен към много малък брой избрани хора. Тези имейли са изключително реалистични и трудни за откриване. Те често изглеждат като че са изпратени от някой познат или колега, друг служител или дори шефа ви. Имейлите изглеждат реалистични, тъй като те могат да използват един и същи жаргон като този,

Измама Изпълнителен Директор

който вашите колеги използват, могат да използват логото на вашата организация или дори официалния подпис на изпълнителни директори. Тези имейли често създават огромно чувство на неотложност, като искат да предприемете незабавни действия и да не казвате на никого. Целта на кибер престъпника е да ви накарат да направите грешка от бързане. Ето три най-общи сценария:

Измамата Изпълнителен директор е мощна атака способна да прескочи повечето защити. Най-добрата защита сте вие самите.

- **Банков трансфер**: Кибер престъпниците търсят пари. Това означава, че те изследват и откриват кой работи в екипа по финанси на вашата организация. Престъпниците тогава измислят и изпращат съобщение в което се представят за шефа ви. Имейлът казва, че е спешно и че трябва да се преведат пари в определена сметка.

- **Данъчна измама**: Кибер престъпниците искат да откраднат информация за колегите ви, така че биха могли да се представят за служители от отдела по данъчни измами. Проучват вашата организация и определят кой обработва информацията за служителите, например, някой в човешки ресурси. От там, кибер престъпниците изпращат фалшиви имейли, преструвайки се на висш служител или може би някой от правния отдел, който иска определени документи да му се предоставят веднага.

- **Представяне за адвокат**: Не всички атаки за CEO измами включват само имейл; могат да се използват други методи, като телефон. В този сценарий, престъпниците започват като ви изпращат имейл преструвайки се на високопоставен мениджър, който ви уведомява, че след малко ще ви се обади адвокат по спешен въпрос. След това престъпникът ви се обажда като се представя за адвокат. Създава огромно чувство за спешност, като говори за неотложни поверителни въпроси. Чувството за неотложност ви подмамва да действате веднага.

Как да се предпазим

И така, какво можете да направите за себе си и за защита на вашата организация? Здравият разум е най-добрата защита. Ако получите съобщение от шефа си или от ваш колега, което не ви звучи както трябва, може да е атака. Подсказките могат да включват огромно чувство на неотложност, подпис, който не изглежда правилно, определен тон, който никога не бихте очаквали или пък име, използвано в имейла, което е различно от това на човека, който

Измама Изпълнителен Директор

всъщност ви се обажда. Друга подсказка би била нападателят да използва имейл адрес или телефонен номер, които никога не сте виждали преди, или може би да използва имейл адрес много подобен на този на вашия колега или шеф, но все пак не съвсем същият. В случай на съмнение, обадете се на човека на доверен телефонен номер или се срещнете с него (не отговаряйте чрез електронна поща) и проверете дали той е изпратил имейла. Никога не заобикаляйте правилата или процедурите за сигурност. Вашата организация може да има политики, които определят правилните процедури за разрешаване на прехвърлянето на средства или споделянето на поверителна информация. Исканията, които се опитват да заобиколят тези политики, независимо от техния очевиден източник, трябва да се считат за съмнителни и да бъдат проверени преди да се предприемат някакви действия. Ако получите такова искане и не сте сигурни какво да правите, свържете се с вашия ръководител, помощния отдел или екипа по информационна сигурност.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на securingthehuman.sans.org/ouch/archives.

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

Ресурси

Социално инженерство:	https://securingthehuman.sans.org/ouch/2014#november2014
Фишинг:	https://securingthehuman.sans.org//ouch/2015#december2015
Зловреден софтуер:	https://securingthehuman.sans.org/ouch/2016#march2016
Двустъпкова оторизация:	https://securingthehuman.sans.org/ouch/2015#september2015
Съвет на деня:	https://www.sans.org/tip-of-the-day

Редакторски колектив: Бил Уайман, Уолт Скривенс, Фил Хофман, Боб Рудис
Превод: Николай Дачев и Радослава Несторова