Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

Фишинг

Преглед

Електронната поща е едно от главните ни средства за комуникация. Ние я използваме не само ежедневно за работа, но също така, за да поддържаме връзка със семейството и приятелите си. Освен това електронната поща е начинът по който повечето компании предоставят онлайн услуги като потвърждения за онлайн покупки или наличие на банковото извлечение. Тъй като толкова много хора по света зависят от електронната поща, тя става един от главните методи за атака използвани от кибер престъпниците. В този бюлетин разясняваме фишинга като често срещан метод за атака и действията, които да предприемете за безопасно използване на електронна поща.

Гост-редактор

Д-р Ланс Хейдън е управителен директор на Бъркли Рисърч Груп. Като експерт по култура и поведение в сигурността той е автор на книгата People-Centric Security: Transforming Your Enterprise Security Culture издадена от McGraw-Hill. Можете да го намерите на www.linkedin.com/in/drhayden.

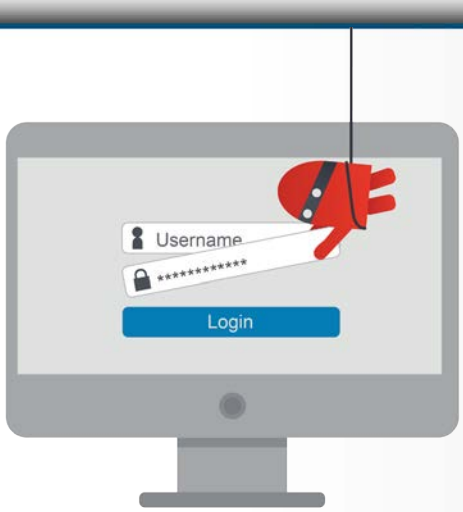
Фишинг

Понятието фишинг се разбира като атака използваща електронна поща или услуга за съобщения (например социални медии), която ви подканва да предприемете действие, например щракване върху Интернет връзка или отварянето на прикачен файл. Ако се подведете по такава атака, рискувате да ви бъде откраднатa важна информация и/или да заразите компютъра си с вирус. Злосторниците се стараят да направят техните фишинг съобщения убедителни. Например, ще направят съобщението да изглежда така сякаш идва от някого когото познавате - приятел или компания на която вярвате и често ползвате. Дори ще сложат логото на банката ви или ще подправят адреса на изпращача, за да направят съобщението да изглежда достоверно. След това злосторниците изпращат тези съобщения до милиони хора. Не знаят кой ще се подведе, единственото което им е известно е, че колкото повече съобщения изпратят, толкова по-голяма е вероятността да успеят. Фишингът е като използване на мрежа за улов на риба – не знаеш колко ще уловиш, но колкото по-голяма е мрежата, толкова по-добър е уловът. Има няколко начина по които злосторниците използват фишинг, за да получат това, което искат.

- **Събиране на информация**: Целта на злосторниците е да се доберат до личната ви информация като пароли, номера на кредитни карти и банкови данни. За да го постигнат, ви изпращат Интернет връзка, която отвежда до достоверно изглеждащ Интернет сайт. Този сайт иска от вас да се удостоверите или да дадете свои лични данни. Тъй като този сайт е фалшив, всяка информация, която въведете отива директно при злосторника.

Фишинг

- **Злонамерени връзки**: Целта на злосторника е да поеме контрол върху вашето устройство. За да го постигне, ви изпраща съобщение с Интернет връзка. Ако я щракнете, тази връзка води до сайт, който атакува устройството ви и заразява системата ви, ако успее.
- **Злонамерени файлове**: Целта на злосторника е същата – да зарази и поеме контрол върху устройството ви. Различното е, че вместо връзка се изпраща заразен файл, например документ. Отварянето му активира атаката, като така дава потенциален достъп на злосторника до системата ви.
- **Измами**: Някой фишинг съобщения не са нищо повече от измами пренесени в дигиталния свят. Те се опитват да ви подведат като твърдят, че сте спечелили от лотарията, преструвайки се на благотворителни организации събиращи дарения или търсещи помощ за превод на милиони долари. Ако отговорите, ще ви бъде поискано плащане за измислена услуга или достъп до банковата ви сметка, при което ще изгубите парите си.



Най-добрата защита е здравият разум. Ако едно съобщение изглежда странно, подозрително или твърде хубаво, за да е истина, вероятно е фишинг атака.

Как да се предпазим

В почти всички случаи отварянето и четенето на съобщението е безопасно. За да проработи фишинг атаката, злосторниците трябва да ви подведат да извършите някакво действие. За щастие има начини да се разпознае дали дадено съобщение е атака, като най-известните признаци са следните:

- Съобщението създава усещане за спешност, изисквайки „незабавно действие“ преди нещо лошо да се случи, като например затварянето на банковата ви сметка. Злосторниците се опитват да ви накарат да действате прибързано, без да се замислите.
- Получавате съобщение с прикрепен файл, който не очаквате или съобщението ви подтиква да отворите файла. Примерите включват съобщения, които твърдят, че прикрепеният файл съдържа информация за предстоящи уволнения, информация за заплатите на служителите или заплашително писмо от данъчната служба.
- Вместо името ви, съобщението използва общ поздрав, като например „Уважаеми клиенти“. Повечето компании и вашите приятели знаят името ви.
- Съобщението изисква лична информация като номер на кредитна карта или парола.
- Съобщението твърди, че идва от официална организация, но има лош правопис и граматика или идва от личен адрес като @gmail.com, @yahoo.com или @hotmail.com.
- Интернет връзката изглежда странно или неофициално. Един трик е да придвижите курсора на

Фишинг

мишката върху връзката без да го натискате, докато се покаже малко прозорче с истинския адрес на тази връзка. Ако връзката в съобщението се различава от тази в прозорчето, не я натискайте. При мобилните устройства това прозорче се показва при натискане и задържане върху връзката. Още по-безопасен начин е да копирате адреса на връзката от съобщението и после да го поставите в браузъра си или направо да го препишете.

- Получавате съобщение от някого, когото познавате, но изказът и използваните думи не са типични за този човек. Ако подозирате, че случаят е такъв, обадете се на изпращача, за да проверите дали наистина ви е пратил това съобщение. За злосторниците е лесно да създават съобщения които изглеждат изпратени от приятел или колега.

Ако прецените, че дадено съобщение е фишинг атака, просто го изтрийте. Най-добрата защита е здравият разум.

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 http://www.securingthehuman.org.

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://www.securingthehuman.org/ouch/2014#november2014
Пет стъпки към сигурността:	https://www.securingthehuman.org/ouch/2014#october2014
Хакнаха ме, какво да правя?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
Ежедневни съвети от SANS:	https://www.sans.org/tip_of_the_day.php

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