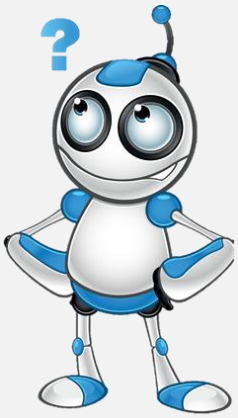
ФИШИНГ АТАКИ

PHISHING



Какво представлява pfishing –риболов?

Злонамерен опит за придобиване на лична информация като потребителско име, парола и детайли на кредитна карта, като извършителят приема чужда самоличност при електронни комуникации.

Как се случва това?

Най-често започва със създаването на дубликат на съществуваща уеб страница на голяма банка или кредитна компания. След това киберпрестъпниците изпращат имейли, чрез които да накарат получателите да отидат към фалшивия уебсайт. Целта е да се подмами доверчивият или недостатъчно просветеният ползвател да съобщи свои пароли, лични или финансови данни.

ФИШИНГ АТАКИ

PHISHING

Варианти на измама

Получателите на този имейл, са помолени да отворят даден хиперлинк, който отваря фалшивия уебсайт. След това от потърпевшите се иска да въведат лична информация (най-често данни от банкова сметка, адрес и телефон). Често се изисква и въвеждане на данните им за вход в оригиналния сайт. Въведената във фалшивия сайт информация се запазва и измамниците могат да я използват.

Друг вариант на измамата е подобна форма за въвеждане на информация, в самия имейл. Потърпевшите са помолени да въведат потребителското си име и парола, както и номера на банковата им сметка. Възможно е измамниците да се опитат да ви подлъжат да свалите троянски кон на компютъра си, от приложение в имейла. След това този вирус събира и изпраща личната ви информация на престъпниците.

Подобни имейли се изпращат на голям брой потребители, като измамниците се надяват да подлъжат малка част от потърпевшите. Най-вероятно получателя дори няма да бъде клиент на избраната от престъпниците институция. Въпреки това те се надяват, че поне малък брой хора ще имат сметки в нея и няма да са запознати с подобни измами. Този вид измама е много изгоден за престъпниците, дори и много малък процент получатели да станат жертви.

ФИШИНГ АТАКИ

PHISHING

Как измамниците използват събраната информация?

Престъпниците могат да използват събраната информация по няколко начина:

1. **Кражба на банкова сметка.**

След като са събрали нужната информация, измамниците могат директно да имат достъп до банковата сметка на потърпевшия. След това могат да извършват транзакции, да пренасочват средства към други сметки и да издават чекове. Най-често престъпниците сменят паролата, за да не може потърпевшия да влезе в сметката си.

2. **Използване на кредитни карти.**

Ако измамниците са откраднали информация за кредитна карта, те могат да плащат стоки за сметка на собственика на картата.

3. **Кражба на самоличността.**

Ако престъпниците са събрали достатъчно лична информация, могат напълно да откраднат самоличността на потърпевшия. След това могат да извършват криминални дела от името на пострадалия. Кражбата на самоличността може да има дългосрочни последици. Понякога на потърпевшите са необходими години да изчистят името си, разрешат възникналите правни проблеми и да изплатят дълговете си.

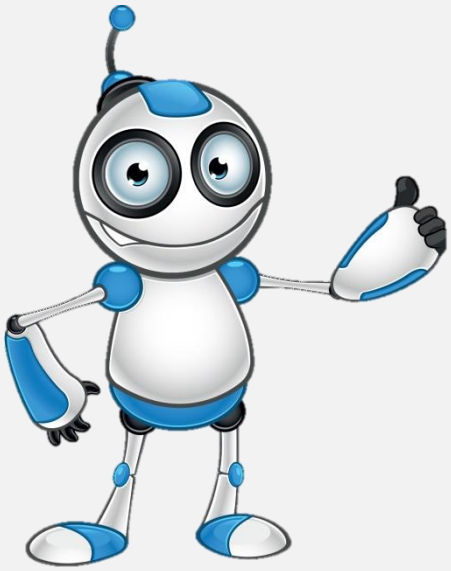
ФИШИНГ АТАКИ

PHISHING

Общи характеристики на фишинг измамите:

Нежелани искания за лична инфорамция.

Смисълът на фишинг атаките е потребителя сам да предостави личната си информация. Ако получите имейл от банка или друга институция, която иска да отворите страница и да въведете лична информация, подходете със силно подозрение. Банките **НИКОГА** не искат лична информация и информация за сметките ви по този начин.



Съдържанието изглежда правдоподобно.

Фишинг измамите са създадени да правят илюзията, че са изпратени от истинска институция. Имейлите могат да съдържат идентично лого и стил, като истинската компания. За да се засили усещането за истинност дори някои от хиперлинковете в имейла водят до истинската страница на институцията. Но този, който води към формата за попълване на информация, препраща към фалшивият уебсайт.

Маскирани хиперлинкове и изпращач.

Линковете във фишинг измамите са маскирани, така че да изглежда все едно препращат към сайта на реалната организация. Адреса на изпращача също изглежда, че идва от домейна на институцията.

Имейлът се състои от картинка, която е хиперлинк.

Някой измамни имейли представляват картинка. Лошото е, че където и по нея да цъкнете, ще бъдете препратени към фалшивия уебсайт.

Общи поздрави.

Понеже се изпращат до много хора, измамните имейли съдържат общи поздрави („Скъпи клиент на …", „Скъпи картодържател" и тн.). Ако някоя институция имаше нужда да се свърже със свой клиент за потвърждаване на подобна информация, най-вероятно щеше да се обърне към него поименно, но както вече споменахме финансовите компании никога не се свързват по този начин с клиентите си.

Многобройни уловки, насърчаващи получателя да предприеме действие.

Във фишинг имейлите е обяснено, че е необходимо потребителят да въведе личната си информация.

Акаунтът на потребителя трябва да бъде потвърден, заради обновяване в системата за сигурност.

Акаунтът на потребителя може да бъде спрян, ако личната информация не е въведена за определено време.

Засечена е подозрителна активност с акаунта на потребителя и той трябва спешно да предостави информацията.

Рутинни процедури за сигурност изискват потребителя да потвърди личната си информация.

ФИШИНГ АТАКИ

PHISHING

Какво да правите, ако получите подобен е-мейл?

НЕ отваряйте хиперлинковете в съдържанието.

НЕ предоставяйте лична информация.

НЕ отговаряйте на имейла и не опитвайте да осъществите контакт с изпращача.

НЕ въвеждайте информация в фалшивия уебсайт, ако той се е отворил.

НЕ отваряйте прикачени в имейла файлове.

Изтрийте имейла.

Какво да правите, ако вече сте били подмамен да въведете лична информация?

Ако вече сте предоставили личната си инфорамция на измамниците, трябва незабавно да се свържете с институцията, от чието име е изпратен имейлът. Важно е да действате бързо, за да запазите банковите си сметки и лична информация. Обадете се на полицията.

ФИШИНГ АТАКИ

PHISHING

Как да се предпазите от фишинг атаки?

Ако имате съмнения относно имейл, изпратен от някоя институция, свържете се директно с нея за потвърждение.

Не кликайте върху линкове в подозрителни имейли. Най-добре ръчно въведете адреса на институцията.

Ако предоставяте лична информация, се убедете че уебсайта е сигурен.

Използвайте антивирусен софтуер.

Обновявайте браузера и операционната си система редовно.