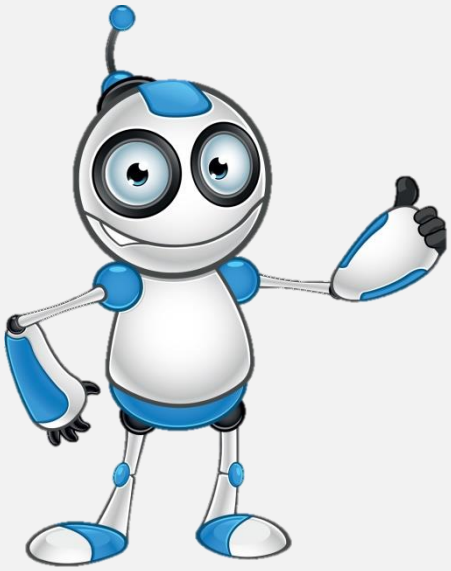
ФИШИНГ АТАКИ

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.