ИНТЕРНЕТ БАНКИРАНЕ, ФИШИНГ И ФАРМИНГ

Съдържание

- Интернет банкиране
- Фишинг
- Спуufинг
- Фарминг
- Разпознаване на измамите

Интернет банкиране

Интернет банкирането може да бъде определено като възможност, осигурена от банкови и финансови институции, която дава възможност на потребителя да изпълнява банкови сделки чрез Интернет. Най-голямото предимство на интернет банкирането е, че хората могат да използват услуги, седейки си у дома, да извършват стопанска дейност. Поради което, на титуляра на сметката не му се налага лично да посети банката. С помощта на Интернет банкиране много сделки могат да бъдат изпълнени от титуляра на сметката. Едни от малкото възможности са проверка на салдо, на скорошна сделка и т.н.

Phishing страници

- Phishing страниците обикновено се разполагат на нечии чужд хостинг акаунт в резултат на хакерска атака. Тяхната цел е да заблудят потребителя, че той се намира на сайта на известна организация, институция или банка, където да въведе информация, която в последствие може да бъде използвана във вреда на потребителя. Най често потребителя се подканва да въведе номерът на своята кредитна карта, но също така има и Phishing страници за които всякаква информация може да е от полза – пароли за достъп до клиентски акаунти, e-mail адреси, персонални данни и т.н. В съвременната Интернет действителност e-mail-а все повече започва да се утвърждава като средство за комуникация и ако даден недоброжелател успее да се добере до паролата за даден e-mail акаунт последствията за неговия собственик биха могли да бъдат катастрофални. Измамниците са се научили да извличат изгоди от всяка попаднала им информация и за това винаги трябва да бъдете много внимателни къде въвеждате и на кой изпращате свята персонална информация.

- Повечето съвременни интернет браузъри предупреждават потребителя, че е на път да отвори страница с подозрително съдържание (phishing page), но все пак на това не може винаги да се разчита . Самия уеб браузър не може сам да прецени дали дадена страница е “phishing” или не. За да бъде определена като такава, страницата преди това трябва да е била докладвана за подобно съдържание.
- Phishing сайтовете най-лесно могат да бъдат разпознати като се провери адресът на сайта в адресната лента на браузъра. Ако смятате, че се намирате на сайта на PayPal, обаче адресът е примерно http://www.paupal.com вместо https://www.paypal.com това е сигнал, че има нещо нередно. В повечето случаи уеб адресът изобщо може да няма нищо общо със сайта, който се представя, т.е. адресът може да е тип http://www.savemymoney.com/payment/clientdata/submit.php . Подобни адреси за phishing страници могат да се видят, когато скриптовете се разполагат на чужд хостинг акаунт в резултата на хакерски пробив, за който собственика на акаунта изобщо не подозира.

Оригинален e-mail, съдържащ линк към phishing страница, насочен срещу потребителите на системата за разплащане PayPal:

*Dear **PayPal** ® customer,*

We recently reviewed your account, and we suspect an unauthorized transaction on your account.

*Protecting your account is our primary concern. As a preventive measure we have temporary **limited** your access to sensitive information.*

*Paypal features.To ensure that your account is not compromised, simply hit "**Resolution Center**" to confirm your identity as member of Paypal.*

- *Login to your Paypal with your Paypal username and password.*
- *Confirm your identity as a card memeber of Paypal.*

Please confirm account information by clicking here Resolution Center and complete the "Steps to Remove Limitations."

**Please do not reply to this message. Mail sent to this address cannot be answered.*

- Когато посетите този линк страницата вероятно отдавна ще бъде изтрита, тъй като подобни страници не успяват да просъществуват повече от седмица. Вероятно Вашия Интернет браузър също ще Ви отправи предупреждение, че сте на път да посетите страница с подозрително съдържание. За съжаление, обаче дори една седмица подобна страница да присъства в Интернет пространството е достатъчно за да бъдат `ужилени` хиляди нищо неподозиращи потребители, чийто банкови сметки бавно ще бъдат източвани в последствие.
- Това е най-дръзкия и най-популярен начин за измама в интернет.
- *Каква е схемата?*

Получава се e-mail в повечето случаи от банка в която жертвата има открита сметка (случва и друга банка да предложи услуга без да се открива нова сметка в нея, а като се посочи сметка от първата банка)
В него се посочва линк на който трябва да се кликне за да се попълнят данните от банковата сметка.
След попълване на данните във фалшивия банков сайт, те се изпращат на измамника.

Фишингът и спуфингът едно и също нещо ли са?

- Спуфингът е имитация на електронно съобщение или на уебсайт, направена от измамници, за да се създаде впечатление, че съобщението или сайтът принадлежат на някой друг. Фишинг атаките обикновено започват с разпращането на непоискани „спуф” съобщения, които изглеждат като изпратени от законна компания. Така че спуфингът е основна част от фишинга, тъй като измамниците Ви карат да вярвате, че електронните съобщения и уебсайтовете всъщност произхождат от компании и организации, на които имате доверие.

Какво е фарминг?

- Измамниците завладяват домейн името на уебсайта на законна компания и прехвърлят потребителите към собствената си „спууфинг” версия на същата Интернет страница. Така те събират личните данни, които вие въвеждате на лъжливия сайт. За съжаление, адресът на страницата изглежда нормално във Вашия уеб браузър и обикновените потребители могат да направят твърде малко срещу фарминга. За да се спре завладяването на домейн имена, е нужно техническо решение. Потребителите трябва да бъдат нащрек и да спазват съветите в рубриката ни за издайнически знаци.

Разпознаване на измамите

- Повечето измами имат следните характеристики:
- Източникът на електронното писмо е ненадежден или непознат за получателя.
- Позовават се на официални източници и са написани така, че да звучат официално.
- Предупреждават за трагични последствия, за да увеличат безпокойството.
- Предупреждават за злонамерен софтуер, който унищожава хардуер.
- Играят си със страховете на повечето хора, като понякога споменават нова, недобре разбирана технология.

- Твърдят, че става въпрос за нов и непознат злонамерен софтуер, непознат на изследователите и компаниите за антивирусен софтуер, без начин да бъде разпознат и без налични инструменти за отстраняването му.
- Съдържат правописни и граматически грешки.
- Съдържат противоречива информация.
- Включват молба да изпратите писмо по електронна поща на всички, които познавате, вместо да предоставят адрес в Интернет, който може да бъде проверен и посещаван.

Трите основни стъпки за защита от измами

- 1) Ако имате съмнения, затворете полученото електронно съобщение и влезте в сметката си от главната страница на онлайн компанията, спомената в съобщението – като използвате нормалния й Интернет адрес *(например* www.ebay.com). 2) Използвайте защитни програми, включително добра антивирусна програма, и ги обновявайте редовно, за да могат те да хващат най-новите вируси и „троянски коне". 3) Използвайте лента с инструменти срещу фишинг (допълнителна редица бутончета, която се появява на Вашия уеб браузър, за да Ви предупреждава за подозрителна дейност).