E-mail фишинг и измамни връзки

Как изглежда фишинг e-mail писмо?

Фишинг e-mail-те служат за кражба на Вашата самоличност чрез интернет пространството - потребителски имена за достъп, пароли, банкови сметки, адреси, електронни пощи и т.н. В повечето случаи те искат от Вас да въведете лични данни или Ви пренасочват към интернет страници или телефони, където да го направите.

Фишинг e-mail-те имат много форми:

- Може да изглеждат като електронни писма изпратени от Вашата банка или финансова институция, компания, с която имате редовни бизнес отношения като Вашият интернет провайдър, или от сайта на Вашита социална мрежа.
- Може да са маскирани като писма от някой, който Вие познавате. Това е така нареченият "spear phishing". Тези писма използват унифицирана форма за масови съобщения от добре известни на "жертвата" компании, учреждения или сайтове като eBay и PayPal, като подателя е човек, който може да е от институцията, в която работи получателят или по принцип човек, чиято работа предполага връзки с клиенти или служители на компанията.
- Фишинг писмата може да съдържат официални лога или други отличителни знаци, взети директно от законните интернет сайтове! Също така може да съдържат и убедителна информация отнасяща се до Вас, която измамниците са намерили в социалните мрежи.
- Друг, много сериозен белег на фишинг e-mail-те е, че могат да съдържат препратки към маскирани, измамни интернет сайтове, които наподобяват на външен вид оригиналните, където искат от Вас да въведете лична информация.

* Пример за маскирана препратка към измамен интернет сайт.

За да направят електронните съобщения дори още по достоверни и привидно законни, измамниците може да поставят препратка, която изглежда, че води към законният интернет сайт(1), но всъщност ще отведе потребителя до измамният интернет сайт(2) или до появяващ се прозорец, който изглежда точно като действителният и официален сайт.