E-mail фишинг и измамни връзки - съвети за избягване на измамите

Съвети за избягване на фишинг измамите

Източник: http://www.antiphishing.org/consumer_recs.html

Броят, както и степента на сложност на фишинг атаките, които се изпращат към потребителите, непрекъснато расте. Въпреки че електронното банкиране и онлайн търговията са много безопасни, винаги трябва да внимавате с даването на личните си финансови данни по Интернет. Работната група за борба с фишинга е подготвила списък с препоръки, които можете да последвате, за да не станете жертва на тези измами.

- Отнасяйте се с подозрение към всяко имейл съобщение, което иска спешно лични финансови данни:
    - Освен ако имейлът носи електронен сертификат за автентичност не можете да сте сигурни, че не е фалшив
    - Измамниците често използват тревожни, вълнуващи или други емоционални твърдения, които са лъжливи, за да накарат хората да отговорят веднага
    - Обикновено искат да им съобщите информация като потребителски имена, пароли, номера на кредитни карти/банкови сметки, номера на осигуровки, рождени дати и тн.
    - Фишинг имейлите обикновено НЕ са персонализирани, т.е. не са предвидени за конкретен човек, но могат и да бъдат такива. Оригиналните съобщения от Вашата банка или компания за електронна търговия по принцип са персонализирани, но винаги трябва да се свържете със съответната компания ако не сте сигурни
- Не използвайте линковете към други страници в имейли или чат съобщения ако подозирате, че съобщението може да не е автентично
    - Вместо това се обадете по телефона на Вашата компания или сами въведете уеб адреса на страницата в уеб браузъра
- Избягвайте да попълвате формуляри в имейл съобщения, които искат Вашите лични финансови данни
    - Информация като номера на кредитни карти или данни от сметки и потребителски профили трябва да се предава само чрез уеб сайтове със сигурна връзка (пред адреса в браузъра трябва да има „http**s**://”) или по телефона

Ако сте свалили вирус или троянски кон (Trojan)

Някои фишинг атаки използват вируси и/или троянски коне, за да инсталират програми, които се наричат "key loggers" на Вашия компютър. С тях те записват всеки един натиснат клавиш на клавиатурата и изпращат тази информация на измамниците. Информацията съдържа всичко, което сте писали- номера на кредитни карти, потребителски имена, пароли, имейли, съобщения, номера на осигуровки и тн. В този случай трябва да:

- Инсталирате или обновите антивирусната си програма, защитната стена (firewall) и програмата за защита от злонамерен/шпионски софтуер (погледнете тук за такива програми http://www.cybercrime.bg/bg/internet/6a0d05/)
- Обновете всички вирусни дефиниции и направете пълно сканиране (full scan) на компютъра
- Прегледайте всички връзки, които минават през защитната стена (firewall)

- Ако защитата е била пробита оправете проблемите и ОТНОВО сменете паролите на акаунтите си (включително системния на компютъра), тъй като паролата от предишната промяна може да е била изпратена на измамниците
- Проверете всички си акаунти/профили! Хакерите може да са влезли в много различни акаунти;