THE BEHAVIOUR AND PERCEPTIONS OF ON-LINE CONSUMERS: RISK, RISK PERCEPTION AND TRUST

Hamid Jahankhani - University of East London School of Computing and Technology

The growth and the expansion of the Internet and the World Wide Web continue to impact society in new and amazing ways. The role of economic commerce has not been as dynamic as some predicted, but has still demonstrated remarkable success and tremendous potential. Any failure to meet some of the expectations may be explained in large part by questions and concerns surrounding existing methods of electronic commerce and of the Internet. A key negative perception centres on the security involved in Internet practice and electronic payment systems. Negative perceptions are then compounded and reinforced by massive media exposure of Internet security incidents. Many consumers still lack the necessary trust in on-line merchants and Internet security procedures and continue to use the Web to simply browse. The types of attack individuals face include confidence-trick or actual encounters calculated to extract bank or personal details, computer spyware that opens on accessing the Internet, enticing users with offers of non-existent free gifts while copying confidential files, and programmes that can infiltrate networks, operating within them undetected, ultimately causing them to crash. Social Engineering is one such method used by an attacker to get information. There are two main categories under which all social engineering attempts could be classified, computer or technology based deception and human based deception.

The technology based approach is to deceive the user into believing that is interacting with the 'real' computer system (such as popup window, informing the user that the computer application has had a problem) and get the user to provide confidential information. The human approach is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked. One of the most effective technology based approach is a scam, called "phishing" as a form of identity theft. This is a technique used to gain personal information for the purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers. This paper provides an overview of electronic commerce and the impact of risk and trust on on line shopping consumer behaviour. Due to the growth and potential of on-line shopping and the lack of academic-based research on Internet-related consumer behaviour, there is a tremendous need for impartial, academic investigation into the
behaviour and perceptions of on-line consumers.

کلمات کلیدی:
Trust, Risk, E-commerce, online shopping, Internet shopping, impact, perceived risk, Social Engineering, Identity Theft, Phishing

لینک ثابت نیت مقاله در پایگاه سیویلیکا:
https://www.civilica.com/Paper-IECWTC02-IECWTC02_012.html