Abstract

Phishing attacks are an important variety of Internet security threat which has been affecting the progress of E-business and E-commerce quite adversely. Safety requirement of e-commerce transactions, quite naturally therefore, has prompted the development of a number of measures meant for countering such attacks.

However, these countermeasures have remained rather ineffective in reducing the attacks, and also the resulting huge losses suffered by victims of such attacks. The present research work is mainly devoted to study and analyze the circumstances under which such attacks take place, as also the behavioural characteristics and responses of Internet users who could be potential victims of phishing attacks. The major part of the study is therefore aimed at getting an insight into the causal factors of inadequacy and ineffectiveness of the countermeasures. A final part of the study has also led to a practical and effective anti-phishing solution suggested by the author.

The first part in this multipart study examines 16 doctoral theses and 358 research papers on phishing mainly to follow the evolution and progress of research in this area detailing the relative distribution of the work among the various publication channels. The findings reveal that the major part of the work has been preventive and advisory in nature.

The second part of the study examines the effect of the available anti-phishing tools and security toolbars provided by the various web browsers and antivirus softwares in detecting phishing attacks. Some experiments were performed in assessing the effectiveness of the tools in detecting the phishing characters of sites specially created for the purpose. These experiments have produced significant results on the natural response of Internet users towards fake websites. Also, significantly, some of the prevalent tools failed to detect the phishing character of some of the sites and passed them as genuine.

The third part of the study examines the importance of awareness as a countermeasure against phishing. To understand the weakness of the human behaviour exploited by the attacker cognitive factors such as attention vigilance and short-term memory were studied as predictor variable along with awareness on phishing, Internet safe practices, Internet skill and other socio-demographic factors to measure the ability to correctly

identify a phishing website. Quantitative research conducted among 621 Internet users with the help of a structured survey questionnaire, and three experiments involving practical interaction with the respondents revealed that awareness on phishing alone cannot stop this menace completely. The results of this study can help researchers to create a suitable model which would enable a better understanding of user's behaviour on the Internet.

The fourth study examines the effectiveness of tougher legal measures as solutions to phishing problems. The study here has indicated that many of the investigations into phishing attacks are stalled midway because neither the e-mail address nor the website can be traced back to a definite owner. These are normally launched through an anonymous open proxy server. Absence of a definite owner makes legal action impossible.

The fifth and the final study presents a new and effective anti-phishing solution - Virtual Browser Extension (VBEx), a web browser plug-in to deter growing number of phishing attacks. Instead of identifying the fake sites, it actually allows secure access to a pre-defined list of websites after verifying the authoritative name server records for the same.

Keywords: Phishing; Identity theft; Social Engineering; Phishing Counter Measures; Phishing Awareness; Internet Safe Practices; Virtual Browser. Information System Security.

***