Chapter 17
Effects of Phishing on E-Commerce with Special Reference to India

Amita Verma
Panjab University, India

ABSTRACT
Phishing is one of the fastest-growing Internet crimes in recent history. Millions of people are affected, and billions of dollars are stolen. Phishing is a technique used to extract personal information from victims by means of deceptive and fraudulent emails for identity theft. As a result of this, the organizations as well as consumers are facing enormous social and economic effects. Phishing is causing two-way damage. This chapter lists the effects of phishing to e-commerce and summarizes techniques available that can be used to prevent phishing with special reference to Indian laws.

INTRODUCTION
Digital infrastructure is rapidly becoming congruent with almost all aspects of modern societies. The inherent nature of the Internet has obliterated all physical boundaries and constructed a worldwide information systems infrastructure. This globalization of information and communication technologies has however posed a problem regarding its security. The increasing decentralization and global interconnectivity has made the system more susceptible to exploitation. Vulnerabilities are not only found in the technical nature of the infrastructure but also in the users themselves. Moreover, the similarity of the infrastructure makes for easy replication of the attack modus operandi at different places.

The faceless nature of the digital infrastructure has made identity theft a natural and extremely attractive avenue. Phishing is just one method of engaging in online identity theft. In phishing, the perpetrators design e-mails and Websites that appear to originate from a legitimate source, thus deceiving the victim into disclosing personal information. “Phishing is a particularly pernicious form of identity theft because it exacts a price on both the individual consumer and on Internet use in general” (Lynch, 2005).

DOI: 10.4018/978-1-4666-4209-6.ch017
DEFINITION

Phishing, also known as “brand spoofing” or “carding”\(^1\) is a process employing the immense capabilities of the Internet to socially engineer people by imitating legitimate forms and methods into imparting their confidential information for purposes of identity theft.\(^2\) “Phishing is a particularly invidious attack on the Internet community because it always involves two separate acts of fraud. The phisher first ‘steals’ the identity of the business, it is impersonating and then acquires the personal information of the unwitting customers who fall for the impersonation. This has led commentators to refer to phishing as a ‘two-fold scam’ and a ‘cybercrime double play” (Stevenson, 2005).

The Delhi High Court opined in National Assn. of Software and Service Companies v. Ajay Sood\(^3\) that,

> Phishing is a form of Internet fraud. In a case of ‘phishing’, a person pretending to be a legitimate association such as a bank or an insurance company in order to extract personal data from a user such as access codes, passwords, etc. which are then used to his own advantage, misrepresents on the identity of the legitimate party. Typically ‘phishing’ scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

The United States Department of Justice defines phishing as, “Criminals’ creation and use of e-mails and Websites-designed to look like e-mails and Websites of well-known legitimate businesses, financial institutions, and government agencies in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords” (Department of Justice, 2004).

“The hacker news group alt.2600 first published the word “phishing” on the Internet in January 1996, although the term was used by computer security trespassers, or hackers, before then” (McNealy, 2008).

The genesis of the word “phishing” is attributed to several sources. It is commonly suggested that the basic etymology arises from the fact that the scammers are “fishing” for confidential information from gullible customers.\(^4\) The orthographic substitution of ‘ph’ for ‘f’ is most likely by analogy to “phone phreaking” (Rosenbaum, 1971), or to distinguish the Internet scam from the sport.\(^5\) Contraction of the term “password harvesting” is another suggested basis of the word “phishing.”\(^6\)

In its initial stages, phishing essentially focused on obtaining passwords of America Online accounts. By 1996, hacked accounts were called “phish”, and by 1997 phish were actively being traded between hackers as a form of electronic currency. With time, the nature of information being phished for has graduated from user account details to access to all personal data.

Phishing Techniques Used by Phishers

The techniques employed by phishers can essentially be grouped under four headings. First, is the Dragnet method, which involves the use of spammed e-mails, Websites, pop-up windows or fake banner advertising bearing falsified corporate identification, that are addressed to a large class of people. This method does not involve identification of specific prospective victims in advance. Instead, it relies on the false information to perpetrate a response from the victims thus enabling identity theft. Nigerian 419 Letters and Work at Home/Reshipping Schemes are extremely common examples of such a technique.

In United States v. Carr,\(^7\) the defendant was found guilty of phishing through unauthorized access devices. Her modus operandi consisted of sending fake e-mail messages to AOL customers directing them to update their credit card and personal information on file with AOL to maintain their accounts.
Related Content

Green Innovation and Ethical Responsibility: Do They Improve Customer's Green Purchase Intentions?
[www.igi-global.com/article/green-innovation-and-ethical-responsibility/211164?camid=4v1a](www.igi-global.com/article/green-innovation-and-ethical-responsibility/211164?camid=4v1a)

Data Protection: A Need of the Hour for Information Technology Enabled Services (ITES)
[www.igi-global.com/chapter/data-protection-need-hour-information/78205?camid=4v1a](www.igi-global.com/chapter/data-protection-need-hour-information/78205?camid=4v1a)

Profits or Employment: Priorities of Future Managers
[www.igi-global.com/article/profits-or-employment/219266?camid=4v1a](www.igi-global.com/article/profits-or-employment/219266?camid=4v1a)

Data-Driven and Practice-Based Evidence: Design and Development of Efficient and Effective Clinical Decision Support System
[www.igi-global.com/chapter/data-driven-and-practice-based-evidence/167299?camid=4v1a](www.igi-global.com/chapter/data-driven-and-practice-based-evidence/167299?camid=4v1a)