Online Phishing and Solutions

4

Ping Wang
https://orcid.org/0000-0003-0193-2873
Robert Morris University, USA

Anteneh T. Girma
University of District of Columbia, USA

INTRODUCTION

Online phishing is a common form of criminal attempt via fraudulent emails, web links and websites to trick online users to surrender sensitive private information, including user names, passwords, social security numbers, credit card numbers, and bank account numbers. Phishing continues to be a primary weapon used by cybercriminals. Phishing is often used as the lead action followed by malware installation or other malicious actions that lead to a data breach. Statistically, 85% of organizations have reported being the victim of a phishing attack (Wombat Security, 2016). Spear phishing email, one example of phishing, was the starting point that led to 91% of successful cyberattacks and the resulting data breach (PhishMe, 2016). In addition, phishing was involved in 70% of all data breaches associated with nation-state or state-affiliated actors (Verizon, 2018).

Phishing attempts may occur in various formats, including email scams, malicious attachments, and fraudulent links and websites. Phishing in nature is a form of social engineering attack that exploits human vulnerabilities of curiosity and lack of awareness and judgment. Individual curiosity and lack of awareness often lead online users to become victims of spoofed and deceptive emails, fraudulent web links and fake websites (Alexander, 2016; Gupta, Arachchilage, & Psannis, 2018). Research on predicting individual susceptibility to phishing shows that certain behavioral traits are correlated to the ability to identify phishing interfaces; it also shows that individuals with greater behavioral curiosity tend to commit more security errors in identifying phishing attempts (Chen, YeckehZaare, & Zhang, 2018).

Online phishing has various types of significant impact on organizational and individual victims. The average direct financial cost of a phishing attack to an organization is over $3.7 million, which is close to the cost of a typical data breach (Ponemon Institute, 2017; Wombat Security, 2015). The costs may include direct loss of productivity and revenue, business disruptions, and costs to contain malware and credential compromises. Additionally, there may be substantial hidden and indirect costs such as damage to corporate reputation and loss of customer confidence as a result of the data breach caused by a phishing scam (Anderson et al., 2012). Phishing scams are a leading cause for individuals to fall victims of identity theft. Over 17 million individuals in the United States alone were victims of one or more incidents of identity theft in 2014, and the majority (86%) of them experienced fraudulent use of their existing credit or bank account information (US Department of Justice, 2017).

DOI: 10.4018/978-1-5225-9715-5.ch056

To combat online phishing, a variety of countermeasures have been proposed, including education and training, improvement of administrative and security policies and practices, as well as technical solutions and software products. This chapter proposes a comprehensive solution to prevent and protect against online phishing. The following sections will define and describe various categories and types of online phishing, explain the theoretical principles for phishing and how each type of phishing works, and propose and discuss a comprehensive set of solutions, mechanisms and best practices to defend users and organizations against online phishing.

BACKGROUND

The term "phishing," with a "ph" from earlier phone phreaking to replace the "f" in "fishing," was first used in 1996 by hackers who were stealing passwords for America Online (AOL) accounts from unsuspecting AOL users, and the first media publications warned consumers about the "phishing" threat in 1997 (Gupta, Arachchilage, & Psannis, 2018; Ollmann, 2017). The earlier concept of phishing was limited to the use of email scams by online criminals to "phish" for passwords and financial data from a sea of Internet users (Ollmann, 2017). But the definition of the phishing has been evolving with various versions. Based on a systematic review of 113 definitions of phishing, Lastdrager (2014) tried to propose a consensual definition: "Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target" (p.8). This definition identified and emphasized the important core concepts of deception, impersonation, information, as well as scalability for mass distribution.

The Anti-Phishing Working Group (APWG), a non-profit international research foundation that specializes in the study of phishing and cybercrime, provides the following definition of phishing that offers a more specific and enlightening focus and directions on the nature and techniques of phishing: "Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" (p.2). The social engineering component of phishing highlights the nature of victimization by exploiting human weaknesses in phishing. The specific technical subterfuge, or mechanisms and methods of deception, may include using spoofed emails, planted crimeware or malware, online interception systems, or phisher-controlled keyboard interception to trick consumers and steal their sensitive information (APWG, 2018).

Social engineering in the context of online crime is defined as "an umbrella term for a broad spectrum of computer exploitations that employ a variety of attack vectors and strategies to psychologically manipulate a user" (Heartfield & Loukas, 2015, p.1). Social engineering primarily targets human users and exploits human psychological weaknesses. The computer exploitations and attack vectors and strategies include examples of technical subterfuge in online phishing to trick and deceive human users. In *The Art of Deception*, Kevin Mitnick, a former master phisher, concluded that the human factor is the weakest link in security and that successful social engineers usually have strong people skills to win and exploit trust from potential victims while most people believe in and behave with trust and love for each other with a low level of suspicion (Mitnick & Simon, 2002). Accordingly, phishing emails and messages often exploit this trust by pretending to be originated from trusted sources, such as friends, government agencies like the Internal Revenue Service, or service providers like banks or credit card companies.

As a critical component of the modern computing systems, humans create most persistent security vulnerabilities as they control system designs and configurations as well as input and output and make decisions on whether or not to click malicious links in phishing emails (Wash & Cooper, 2018). Research on human psychology indicates that online phishing has been gaining popularity due to the flaw in hu-