Chapter 6
Combating the Phishing Attacks: Recent Trends and Future Challenges

Sonia Tasmin
North South University, Bangladesh

Asma Khanam Sarmin
North South University, Bangladesh

Mitul Shalehin
North South University, Bangladesh

A. K. M. Bahalul Haque
https://orcid.org/0000-0002-7942-0096
LUT University, Finland

ABSTRACT

The phishing attack targets the client's email and any other connection medium to illicitly get the user credentials of e-commerce websites, educational websites, banks, credit card information, and other crucial user information. Exploitations caused by different types of cyberattacks result in data loss, identity theft, financial loss, and various other adversaries on both human and infrastructure. Therefore, investigating the threats and vulnerabilities on web applications and analysis of recent cyberattacks on web applications can also provide a holistic scenario about the recent security standpoint. Therefore, in this chapter, phishing attack techniques and their current scenario will be discussed extensively. Moreover, recent phishing techniques will be discussed to understand the severity of this type of attack. Finally, this chapter will outline the proposed and existing countermeasures for protecting users' identities and credentials from the phishing technique.

DOI: 10.4018/978-1-7998-9426-1.ch006

INTRODUCTION

Cyber Security refers to the process of defending cyberspace from threats (Iwendi et al., 2020, Rehman et al., 2020). It is concerned with maintaining, limiting, and retrieving all internet-connected resources from cyber-attacks (Javed et al., 2020, Mittal et al., 2021). The complexity of the cybersecurity domain grows by the day, making it difficult to identify, explain, and monitor the relevant risk events. In this process, some cyber professionals are always trying to protect computer systems from cyberattacks. Nowadays, cyberattacks target corporations, private systems, and various attacks are also increasing day by day. According to the former CEO of CISCO, two types of companies are threatened by cyber security. One has already been attacked, and the other one has not been hacked yet. Cyber-attack is one kind of malicious attack where attackers try to gain data, disrupt digital operations or damage sensitive information in an unauthorized way (Tweneboah-Koduah et al., 2017). Among numerous cyberattacks, phishing has become one of the most threatening offenses in the Internet world. The term phishing was first introduced in 1996, and it has evolved since then (Gupta et al., 2018). It refers to a social engineering crime that aims to seize crucial and personal information such as username, password, bank and transaction card details of users.

The approaches to phishing attack techniques that create a trap for the user over email, SMS, social networking sites, and other websites have evolved over the years. The types of phishing are deceptive, malware-based, DNS-based, and content-injection phishing (Ali, 2017, Chaudhry et al., 2016). The most common path is via Email, where attackers provide the hyperlink to update their information (Halevi et al., 2015). In this case, they create an interface that looks real, and users think the message comes from a trusted sender. As users engage with other works, they do not notice the minor significant differences. As a result, they become phishing victims as they often download malware unknowingly on their computers. On the other hand, phishers can get access to a variety of information with our password. In this case, when a user uses unsecured WIFI in a public place, attackers create a barrier between the visitor and the network using malware to install software that helps transmit the personal data to the attacker (Gupta et al., 2018). There is also an underground market where phishers can purchase and sell their phishing tools and users' valuable information (Ramzan, 2010). Phishers use several phishing tools and techniques such as Email Phishing, Clone Phishing, SMS Phishing, Voice Phishing, Software Phishing, and Websites Phishing. The latest techniques of phishing are WI-FI Phishing, Cross-site Scripting, and Domain Phishing (Singh et al., 2019, Sharma et al., 2019).