**PHISHING ATTACK**

**Executive summary**

In this study the focus is given on the manner in which phishing attack creates problem in maintaining data security and confidentiality. The study emphasizes on the need of innovating new software in order to prevent stealing of vital information that are confidential for any organization. The three variants of phishing attack are discussed in detail along with an outline of the working procedure of such phishing attack. It can also be recommended that the innovation of new software’s can turn out to be positive effect in improvement of the computer system.

**Table of contents**

[1. Introduction 3](#_Toc3212712)

[2. Discussing the three variants related to a phishing attack 3](#_Toc3212713)

[ Spear Phishing 3](#_Toc3212714)

[ Clone Phishing 3](#_Toc3212715)

[ Dropbox Phishing 3](#_Toc3212716)

[3. Working procedure of phishing 4](#_Toc3212717)

[4. Threats received by phishing 4](#_Toc3212718)

[5. Summary 5](#_Toc3212719)

[6. References 6](#_Toc3212720)

1. Introduction

A phishing attack is linked with stealing user data that includes login credentials and improving the card numbers. This procedure goes on when an attacker is trying to get into the trusted entity in stealing data and hacking the computer information. In this study, the main focus is given on how network attack has increased to a great level in many areas. Increasing of threats occurs which turns out to be a weakness of a particular company in storing relevant data. The various techniques used by the attacker in protecting the data is also given emphasizes. It also discusses the threats that the computer system faces in innovating new procedures for the improvement of the information.

2. Discussing the three variants related to a phishing attack

* Spear Phishing

This procedure is considered as an electronic communication scam that is targeted towards a specific system, business and organization. According to Alsharnouby *et al.* (2015, p.70), many times stealing of data occurs in order to improve the malicious purposes which are avoided by cybercriminals by installing malware software on a computer that are targeted by the attacker. In order to protect the spear phishing attack, the traditional security system is installed for improving and avoiding the attacks that cause a problem.

* Clone Phishing

Clone phishing is considered a fraud attack that comes under the procedure of social engineering. Rittenhouse *et al.* (2016, p.250) opined that clone phishing is targeted based on specific organizations and individuals in order to get identical and original mail from different sources. All emails are spoofed in order to make the organization believe that it has come from the original sender.

* Drop box Phishing

Phishing on the concept of Drop box helps in exchanging the unlicensed software for preventing hacking and storing important information from relevant sources. Drop box helps in allowing users to store share and organize information collected from various resources. In order to protect drop box phishing-based attacks on the system, it is necessary to install anti-hacking features for the betterment of the organization in storing information.

3. Working procedure of phishing

Phishing is considered as a significant problem that involves fraudulent email and websites that prevent revealing private information. Phishing helped people in gaining knowledge about various security measures in order to get information from lost sites. Wu *et al.* (2016, p.6679) stated that phishes or attackers destroy or exploit to conduct and render mechanism for the improvement of the system and the organization that is not attacked with fraudulent attackers such as phishing which is influenced by malware software. In order to improve the mechanism, new software needs to be made for the improvement and safety of systems in different organizations.

4. Threats received by phishing

Phishing attacks are at the top of cyber attack challenges for business and healthcare organization. According to Wu *et al.* (2016, p.605), it is identified that 92% email delivered is from the malware software. This software sometimes prevents phishing attacks to systems in meeting challenges faced by the organization. The threats of avoiding phishing attack include staying aware, running test, quality matters in innovation of a program and credential threats.

|  |  |
| --- | --- |
| **Threats** | **Analysis** |
| **Staying aware**  | As explained by Alsharnouby *et al.* (2015, p.75) concentrating on conditioning users in order to report questionable emails for better improvement of the system and avoid a threat.  |
| **Running tests**  | Jensen *et al.* (2017, p.600) defined that engaging in the phishing simulation is based on active threats. It also focuses on the threats that the business or the organization faces. |
| **Quality matters in innovating programs**  | For improving the phishing awareness program quality and quantity of products is considered as an important factor. |
| **Credentials threats**  | This procedure helps in remaining active and avoiding the threat that creates difficulties in extracting data from relevant resources. |

**Table 1: Threats of phishing attack**

(Source: Influenced by Wu *et al.* 2016, p.6680)

5. Summary

Phishing is considered as an online identity that aims at stealing information from various resources which are sensitive in its composition. Attackers are employing a large number of technical and spoofing techniques in order to improve the phishing attack and collect relevant information from different sources. In this study, it is seen that the three variants are playing a vital role in improving the systems from getting attacks from unwanted sources.

6. References

Alsharnouby, M., Alaca, F. and Chiasson, S., (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, pp.69-82.

Chaudhry, J.A., Chaudhry, S.A. and Rittenhouse, R.G., (2016). Phishing attacks and defenses. International Journal of Security and Its Applications, 10(1), pp.247-256.

Gupta, B.B., Tewari, A., Jain, A.K. and Agrawal, D.P., (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), pp.3629-3654.

Jensen, M.L., Dinger, M., Wright, R.T. and Thatcher, J.B., (2017). Training to mitigate phishing attacks using mindfulness techniques. Journal of Management Information Systems, 34(2), pp.597-626.

Wu, L., Du, X. and Wu, J., (2016). Effective defense schemes for phishing attacks on mobile computing platforms. IEEE Transactions on Vehicular Technology, 65(8), pp.6678-6691.

Wu, M., Miller, R.C. and Garfinkel, S.L., (2016). Do security toolbars actually prevent phishing attacks?. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 601-610). ACM.