Journal of Forensic Sciences
And
Criminal Investigation
ISSN: 2476-1311

Juniper
PUBLISHERS
key to the Researchers

Review Article
Volume 3 Issue 5 - July 2017
DOI: 10.19080/JFSCI.2017.03.555629

J Forensic Sci & Criminal Inves
Copyright © All rights are reserved by Doris Karina Oropeza Mendoza

The Scam in the Ciber space: Phishing

Doris Karina Oropeza Mendoza*

Independent Research Professional, Mexico

Submission: July 19, 2017; **Published:** July 28, 2017

***Corresponding author:** Doris Karina Oropeza Mendoza, Doctor in Public Law by Legal Research Institute of the Universidad Veracruzana, Mexico, Tel: +521 22 88 26 93 15; Email: doropeza1012@gmail.com

Abstract

Cyberspace is an environment that has been depleted by cyber-criminal behavior that carry out crimes that affect users of the web; one of these behaviors is phishing, which has cost millions of dollars in losses for companies and individuals. This text addresses a brief analysis of this scam.

Keywords: Cybercrime; Phishing; Email malicious; Cyber security

Introduction

Cyberspace is the technological platform that currently supports financial, commercial, economic, social, cultural, entertainment, among many others; The information circulating on the Internet is highly sensitive and even confidential for its users, representing, for example, for various companies, a fundamental asset or a product, which are converted into amounts that are millions of dollars, therefore, information must be highly protected against attacks by Cyber-criminals who using criminal strategies can perpetrate the theft of information and use it for criminal purposes, mainly in pursuit of an economic benefit. One of these criminal strategies is the illegal activity known as phishing, attacks of this behavior have spread throughout the world, and there are no limits for attackers in terms of companies or users that are affected by such activity, Have revealed attacks on large companies like Apple, Amazon, among others.

What is the phishing?

The Anti-Phishing Working Group defines: Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials[1]. The word "phishing" was first posted in a Usenet group dedicated to American Online el 2 de enero de 1996[2], after an attack that the company underwent AOL. Phishing is a form of cyber-crime, which occurs "when the perpetrator sends fictitious e-mails to individuals with links to fraudulent websites that appear official and thereby causing the victim to release personal information to the perpetrator"[3]. This cybercrime is carried out through the knowledge of software development experts, who create a website with a design similar to the one the victim believes the victim accesses, another form of cybercrime is the hacking of the original website for Introduce software to commit fraud. E-mail is the most common way to launch "the hook", which is done through a message whose data seem authentic inviting victims to open a link that directs the website to perpetrate the wrong, messages are so Well designed that seem reliable information for the users causing them to "bite the hook" and open the website to which they are directed, once the above has occurred the illicit is concretized by stealing valuable and sensitive information from the victim or deceiving her to contribute Confidential data, thus cyber-criminals carry out the commission of other offenses that start with identity theft, and / or identity theft. Attention to the above, we can point out that phishing is a primary crime that is destined to carry out other crimes that mostly concur in patrimonial robberies, for example, obtaining bank details for theft of money through Internet banking or the purchase of products or services via the Internet.

The Problem

According to the report of The Anti-Phishing Working Group (AWPG), phishing attacks increase year by year, in 2015 registered 227,471, while in 2016 recorded 255,065, [4] 57% of attacks worldwide Were made against four Web giants: PayPal, Yahoo !, Apple, and Taobao.com, with China being the most affected country with 25% of the attacks. According to the same report, the ranks of affected web industries are shown as follows:

eCommerce & Software / SaaS 30%, Banking & Financials 25%, Social Networking & email 19%, Money Transfer 18%, ISP, Hosting & Cloud 4%, File Storage / Transfer 2%, Government 1%, Other 1, Gaming 0% [5].

This year, on May 3, users of the Google Docs, from Google Inc., were victims of one of the most severe phishing attacks known to date, some journals define a sophisticated phishing attack [6].The social networking has been targeted by hackers to attack its users and steal their passwords and even bank details, as explained by the website "The Next Web":"Polish internet swindlers have cooked up an elaborate scam that involves taking over your Face book profile to ransack your bank account and swiftly transfer the stolen funds to anonymous Bit coin wallets"[7]. The above data are alarming figures that give us an overview of the seriousness of this criminal activity in the digital environment, economic losses are millionaires and the safety of users has been altered, before this the need -urgent- of attention and The union of efforts by governments, companies, technical experts in software and Internet and users of the network, to diminish the success of the attacks perpetrated.

Running Phishing

At the beginning of this document a description was given of how a phishing attack operates, however, it is convenient for this document to make an analysis of the routes that cyber victims can face:

a) Route one: Once the victim clicks on the malicious email link it is directed to a fake website whose Uniform Resource Locator (URL) was assigned to a web address whose domain name registration was initially created for criminal purposes. In this case the design of the websites is similar to the original site of the company to which the victim creates access, so the users do not notice the fraud to which they have been redirected, and with confidence they give access to the information that is Required without warning of deception, until the data has been used by cyber criminals.

According to the report of The Anti-Phishing Working Group (AWPG), in the year 2016, 195,475 domain names were used for this criminal act, of which 95,424 were registered maliciously, that is, intended specifically to commit the robbery [8].

b) Route two: In this second way of operating phishing, the malicious email "invites" the cyber victim to address a link that leads to a website, which is original company, however said site has been hacked, the Phishers has introduced on the website a software where victims will be directed directly to commit the robbery translated into the permission to access their accounts and the data in it as contacts, bank details, work or personal information, and even theft of the password To enter all user information.

This route was followed by phishers in attacking users of Google Docs, regarding Alex Johnson of NBC News describes: *The worm — which arrived in users' inboxes posing as an email from a trusted contact — asked users to check out an attached "Google Docs," or GDocs, file. Clicking on the link took them to a real Google security page, where users were asked to give permission for the fake app, posing as GDocs, to manage users' email account* [9]. In 2016 of the domains noted above as being used for phishing attacks, 100,051 correspond to sites that were hacked by phishers [10].

To say of Infosec Institute, another route used by the phishers to commit the robbery is the Pop-Ups

c) Messages: that is: *one of the easiest techniques to conduct successful phishing scams. They allow hackers to steal login details by sending users pop-up messages and eventually leading them to forged websites through these pop-ups. A variant of phishing attacks, also known as "in-session phishing," works by displaying a pop-up window during an online banking session and appears to be a message from the bank* [11].

Damage Caused By Phishing

When a phishing attack succeeds, criminals carry out the following objectives [12]:

I. Using data to access a victim's account and withdrawing money or making an online transaction, e.g. buying a product or service.

II. Using data to open fake bank accounts or credit cards in the name of the victim and using them to cash out illegal checks, etc.

III. Using the victim's computer systems to install viruses and worms and disseminating phishing emails further to their contacts.

IV. Using data from some systems to gain access to high value organizational data such as banking information, employee credentials, social security numbers, etc.

The damages caused by these attacks are multiple and varied however there are two main classifications: economic damages and moral damages. In the first case the victim can lose large amounts of money, or valuable information that represents fundamental assets especially in the case of companies and people who were victims of the scam. In terms of moral damages, affectations can reach a person's reputation due to a misuse of the identity that has been stolen, however affectations for companies even entail the collapse of the trust that the brand of a company has Achieved over long periods of time and with great efforts, victims of phishing, reduce the trust in the company that phishers have used to carry out the scam.

The Fight Against Phishing

Phishing is a crime whose characteristics can reach international levels, overcoming borders and legal limits, given that cybercriminals can be physically in China and cyber-victim in the United States, so a legal context is necessary in which There is harmony in the legislation of the countries so that the prosecution of the crime guarantees the reparation of the victim's injury and punish the criminals. In this context, the Budapest Convention is the international instrument regulating cybercrime. It was signed by Member States and non-member States of the European Union such as the United States of America, Japan, South Africa and Canada. It was created before the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation; This agreement in articles 2, 4 and 8 consider elements that are part of phishing, so that countries that have harmonized their domestic legislation with this agreement have a legal framework that sanctions such behavior and sets the rules for their pursuit.

Likewise, cybercrime and secondary crimes committed in the United States violate various statutes, such as: identity theft (18 U.S.C. § 1028(a)(7)), wire fraud (18 U.S.C. § 1343), credit-card (or "access-device") fraud (18 U.S.C. § 1029), bank fraud (18 U.S.C. § 1344), computer fraud (18 U.S.C. § 1030(a)(4)), and the newly enacted criminal offenses in the CAN-SPAM Act (18 U.S.C. § 1037). The best way to prevent crime is to establish prevention measures, to say of United Nations Office on Drugs and Crime, some strategies are: restriction of the publication of critical identity related information, to data breach notification requirements and a better protection of large databases[13].

Conclusion

The protection of information to avoid being obtained by criminals may consist of locks such as the application of a PIN Personal Identification number) or biometric information, which greatly reduces the theft of personal data, but above all the education of cyber -population is a powerful strategy to reduce phishing attacks, it is critical that users know the modus operandi of this type of crime, and warning signals to avoid falling into the delusion of cyber criminals, and minimize the possibilities Of success of the attack.

References

1. Anti-Phishing Working Group (2017) Phishing Activity Trends Report 4th Quarter 2016. p. 2.
2. Moramarco, Stephen (2016) Phishing Definition and History.
3. Kratchman Stan, Smith Jacob L, Smith Murphy (2008) The perpetration and prevention of cybercrime. Texas A&M University-Internal Auditin 23(2) pp. 3-12.
4. Anti-Phishing Working Group (2017) Global Phishing Survey: Trends and Domain Name Use in 2016. APWG p. 1-48.
5. Idem, p. 7-9.
6. The guardian (2017) Google Docs users hit with sophisticated phishing attack in their inboxes.
7. The Next Web (2017) Thieves use Facebook tricks to steal your money and turn it into Bitcoin. by MIX - 26 days ago in SECURITY.
8. Idem, p. 5.
9. Jhonson, Alex (2017) Massive Phishing Attack Targets Gmail Users. NBC News-Tech.
10. Anti-Phishing Working Group, op cit. nota 5, p. 6.
11. Mohsin, Tahshina (2016) Phishing Tools and Techniques.
12. Mohsin, Tahshina (2016) Phishing as a risk (Damages from phishing). Infosec Institute.
13. United Nations Office on Drugs and Crime (2011) Handbook on Identity-related Crime, New York, USA, pp. 1-350.

DOI: 10.19080/JFSCI.2017.03.555629

How to cite this article: Doris K O M. The Scam in the Ciber space: Phishing. J Forensic Sci & Criminal Inves. 2017; 3(5): 555629. DOI: 10.19080/JFSCI.2017.03.555629.