Natalie Vasquez, Christian Moore, Sergio Quijano

April 5th, 2018

Business Information Systems and Analytics

Professor Reagan

Phishing

When it comes to sensitive information regarding Credit Card details or even passwords and usernames, phishing is a big problem with all of those sensitive things. Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. For example, people can use phishing to get into your bank details and use and steal your money for their own malicious benefits.

Phishing started to become well known in the mid 1990's due to a hacker and spammer by the name of Khan C Smith. Though in the early 2000's is where more phishing situations have occurred. Such as between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately US$929 million. United States businesses lose an estimated US$2 billion per year as their clients become victims. Phishing is not only just a small problem, it is actually a problem that has even caused issues for the United States business that costs them millions of dollars lost.

When it comes to phishing, there are different types that affect a variety of people in different ways. There is Spear Phishing that is directed at specific individuals or companies to take money. When it comes to Spear Phishing the attacker can search up personal information

about the victim to get a higher success rate with getting their personal information. An example of it is that a Threat Group used spear phishing to target emails linked to Hilary Clinton's 2016 presidential campaign. As of 2018 after the campaign has ended, you can see that the emails affected her campaign to lose the election to Republican nominee Donald Trump.

Another example of Phishing is Clone Phishing, and what that is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address or addresses taken and used to create an almost identical or cloned email. For example, there can be emails that ask for you to donate to a good cause, let's say a child in a third world country. When they ask for you to donate they ask for your card information and pin which can give them access to your card and steal your money.

Another type of phishing is referred to as Whaling, which are several phishing attacks have been directed specifically at senior executives and other high-profile targets within businesses. Now these kinds of phishing attacks go for the upper-management and involves a company-wide concern that is false. This has the manager click the link so then they can install a special software to view the manager's computer systems and hack into them. Which can cause a huge problem for companies especially when it comes to finances and secrets of the company that the outside world can not know.

With Phishing you have to be very careful because hackers and scammers can get into anything that contains any personal information and can even try to steal an identity. Phishing has been a big problem when it comes to all the new technology coming out. With all this new technology, people have easier access to gain private information easily, that includes social security numbers and credit card numbers. All this new technology is giving the hackers easier

access to all this stuff and which is why phishing is occurring more often to innocent people and higher ups in companies.

When scammers and hackers want to get into the personal information, now and days they use the new technology and usually forge things, especially FBI subpoena emails. Hackers are all over even from other countries and they are getting smarter and smarter everyday with new ways to hack into people's personal information that sometimes it is pretty impossible to tell what is fake and what is real. Especially when a lot of emails, texts, and phone calls sound so real and convincing, nobody knows what to trust anymore when it comes to all of this.

But there are ways that you can avoid being a victim of phishing for now and for the rest of your life. One way is to think before you click especially if it does look fishy. Though if it does not look at all like a good idea the best thing to do is to not click the link and avoid it, especially delete it so you never see it again. Another way to avoid phishing schemes is verify a site's security, by this I mean to look up the site online and see if it has any bad reviews and comments about it. Cause if other people have had bad issues with the website and had problems with them trying to trick them and be able to write about their experiences online not only shows that you aren't the only, but also gives you a heads up on it all to know not to click on the link and give up your personal information.

Another way is to keep informed about Phishing techniques, be sure to keep up with the news about any phishing scams that happen and what they did and how they did it. You will be surprised by how many stories actually come up about phishing because in today's generation with all this technology, phishing does happen every so often especially to the older generation that don't know any better and don't know much about technology.

When it comes to Phishing prevention the best thing to do is be aware and always alert when receiving a notification about something suspicious. Don’t fall for anything that has you release your personal information and can cause negative effects in the future. The best advice is to just be aware and be known of what phishing is and how it is done especially with all this new technology coming out.

Works Cited

- Phishing. (2018, April 03). Retrieved April 05, 2018, from https://en.wikipedia.org/wiki/Phishing
- "Phishing" Fraud: How to Avoid Getting Fried by Phony Phishermen. (2013, September 05). Retrieved April 05, 2018, from https://www.sec.gov/reportspubs/investor-publications/investorpubsphishinghtm.html