Reflective Project

Is it ethical for "phishers" to obtain personal information?

3/24/2014

Table of Contents

Ethical Question

The ethical question that I will be answering in this reflective project is, it is ethical for "phishers" to be able to obtain personal information?

Introduction

Phishing has been around since 1995, and has been a huge problem ever since it started. Phishing is the process where a targeted individual is contacted by email or telephone by someone acting as if they were a legitimate company to lure an individual into giving out personal information. The different kinds of information these "companies" are getting are banking information, credit card information, and various passwords. Identity theft and financial loss are the results of phishing. There are many different perspectives when looking at this ethical dilemma.

Victim

To the victim, it would be considered very unethical for someone to obtain their own personal information. It is an invasion of privacy and can and the victim can lose very personal information that can lead to identity theft. It can be very hard to tell whether the website is legitimate because phishers are starting to make these fake emails realistic. More and more people are falling for these scams. Kaspersky Lab, which is a security company, reported in an article, released on June 20, 2013, that 37.3 million users experienced phishing attacks in the last year. Services such as, Yahoo!, Google, Facebook and Amazon were most attacked by phishers because they made fake versions of these websites.

Phisher

To the phisher, this topic would be ethical because they think that it is right for them to get this personal information because it is there form of a job. As long as it benefits them they would not think that the issue is unethical. There are different types of emails phishers use. For example, a phisher can send an email saying that the "victim" has won an iPhone and the fake website asks for information that the phishers use to steal information. Another example is that the phisher will send you some kind of urgent email and they will tell you that you need to update your information quickly or else your account will be suspended. Phishers also use emails that use generic names, if they do not use your real name it is most likely a scam. In the Kaspersky Lab article, American Express, PayPal, Xbox live, and Twitter are some of the top 30 most targeted sites. During the year of 2012 to 2013, phishers launched attacks that affected around 102,100 people each day.

Reflection

In the beginning I had different thoughts about what phishing was. I thought that it was an easy thing to get rid of; I thought that nobody would be dumb enough to fall for these scams, and I thought that it was not a really big problem, but that is the total opposite. Many people are falling for the scams that the phishers are sending them and it is not an easy thing to get rid of, once that person has your information there is no way for you to erase it or take it away from them. It is a huge problem in the internet there are many cybercrimes being committed. I was not really sure if it was an ethical issue because I thought that it was not a big deal but after doing my research I found out that it is very unethical that phishers are obtaining personal information.

Although to the phisher it may be ethical to take information from someone because it benefits them, but it is unethical for them to steal that kind of information because it affects someone in a way that puts them in danger. This is a big problem in the world of technology. It is a cybercrime that needs to be stopped.

Conclusion

The amount of people being affected by phished is increasing drastically each year. In an ZDNet article it said, "According to a recently released report, based on a sample of 3 million users collected over a period of 3 months, approximately 45% of the time, users submitted their login information to the phishing site they visited." There will always being phishing you cannot get rid of it, you can only prevent it. If the government would like to prevent it they would have to have more enforcement on the internet monitoring these scams. The government can also let the people be aware of scams like these. They can give us very helpful tips to help people from being scammed by these phishers. In the point of view to the victim being scammed by phishing is very unethical because it is an invasion of privacy and can lead to identity theft and financial loss. Although it may seem ethical to the phisher, it is wrong for them to steal people's personal information. The things that the phisher are doing are illegal and the government should try their very best to prevent phishing.

Bibliography

Danchev, Dancho. "How Many People Fall Victim to Phishing Attacks?" *ZDNet*. ZDNet, 4 Dec. 2009. Web. 31 Mar. 2014.

"History of Phishing." *Phishing.org*. N.p., n.d. Web. 29 Mar. 2014.

Press Releases. "Kaspersky Lab Report: 37.3 Million Users Experienced Phishing Attacks in the Last Year." *Kaspersky Lab Report: 37.3 Million Users Experienced Phishing Attacks in the Last Year*. Kaspersky Lab, 20 June 2013. Web. 31 Mar. 2014

"What Is Phishing?" *Phishing.org*. N.p., n.d. Web. 29 Mar. 2014.