Internet Fraud

No one could have imagined how the Internet transformed the lives of people in the 21st century. At the early stages of development, the Internet was a communication tool that was supposed to make lives easier for a few researchers or engineers. No one thought that the Internet could become a communication tool enjoyed all over the planet. In addition, the Internet evolved into something more than a communication platform. Social media sites like Facebook and YouTube characterizes the Internet as community builder, a way to share ideas, and a way to get entertainment as well as productive work. However, there are also unintended consequences and the chief among them is white-collar crime and Internet fraud. An example of some of the illegal activities that unscrupulous people can commit through the World-Wide-Web is to use the Internet to harm others through identity theft. In addition, people all over the world are also grappling with the impact of cyberbullying. It is important to learn more about white collar crimes based on Internet fraud as well as cyberbullying in order to develop appropriate policies and regulatory measure in order to reduce the incidence of the said problems.

The Unintended Consequences of the Internet

The misuse of the Internet produces different types of problems. It can be as irritating as unsolicited messages, commonly known as Spam. This type of messages are sent using messaging systems from popular sites like Yahoo and Gmail. However, these seemingly innocent messages can become the seed or starting point of more serious illegal activities. When it comes to non-criminal acts, spamming is an activity that annoys people. In some cases, the messages are offensive or wastes people's time. Some of the messages are inappropriate and may cause a great deal of distress depending on the recipient of the messages. For example, pornographic content can easily create emotional and psychological distress to minors.

Spamming enables unscrupulous people to launch more sinister attacks. For example, the initial stages of an identity theft may originate from the receipt of spammed messages (Abate, 2008). Once the computer user opens or use the file embedded in spam messages, they could be in real trouble. Identity theft is a serious problem because it uses the personal information of the victim in order to gain access to personal and confidential items, such as financial holdings and access into secured areas or critical areas in an office or manufacturing facility.

Aside from “spam messages” another problematic byproduct of the use of the Internet is “phishing”. It is important for business owners and corporate leaders to invest in anti-hacking or illegal surveillance of the company's assets. It is also important to point out a variation in the mode of entry using phishing. This is difficult to control and manage because the user of the computer is deceived into thinking that he or she has access. Phishing works due to the clever strategy of studying human

behavior.

As discussed, identity theft is the first step in the attempt to create bigger crimes. However, “phishing” uses sophisticated skills in creating a message that tempts a person to click on an email or open a file. For example, the creator of a “phishing” type of message could create a message that talks about company politics or a problem that a co-worker wants to talk with others. This type of messages makes it difficult for the average person to ignore. This is a good example why developers of “phishing” are knowledgeable about human behavior. It is important to educate people about the nature of phishing, because in the early stages, the attacks may come,as innocent and non-threatening lies. In a typical spamming, the message may not sound dangerous at first. At the end, however, once the victim clicks a file he or she activates a virus or malware that spies on computers or damages computer hardware.

Phishing and Cyberstalking

While conventional types of phishing is a nuisance to the general public, it is also important to point out that serious types of phishing had been developed. Consider for instance the problem caused by “spear phishing”. Instead of sending out thousands of emails hoping to get one person to click on the message, this is a much more personalized approach that has been proven to be really effective even against veteran security professionals. Spear phishing, is actually an attempt to send messages under false pretenses.

It is imperative to invest in catching criminals that are linked to phishing, because this illegal activity can evolve into something that is more problematic. For example, phishing based on identity theft can lead to credit card fraud. Credit card fraud is something that can come out from a successful phishing attempt. In the past, credit card fraud was limited to accessing funds using the ATM or in the case when wallets and purses had been stolen. However, credit card fraud in contemporary times involves the use of the Internet. This is made possible by the prevalence of online shopping. Aside from online shopping, users utilize the power of the Internet to pay bills and acquire other items online.

In addition to credit card fraud, people are also victimized by cyber-bullying or cyberstalking. Merritt defines cyberstalking, otherwise known as online stalking, as the use of technology, especially the internet, to harass someone. Common examples of cyberstalking practices include unnecessary monitoring, threats, false accusations, data destruction and manipulation, and identity theft. Child exploitation is also regarded as a cyberstalking act, whether it is defined as a sexual act or defined another way.

Mediums used in implementing a cyberstalking exercise include instant messages, emails, phone calls and any other communication devices. Interestingly enough, research show that cyberstalking perpetrators are sometimes known to their victims. There have been numerous cases wherein the victim and the perpetrator know each other. In many cases, the victim and perpetrator were former lovers or friends. In other words, people had become more vulnerable the moment they become dependent on the Internet for communication and social needs.

Conclusion

It is important to focus on “spam messages” and “phishing” because the most dangerous threat is the one that people did not expect is coming. Phishing for instance can appear as an innocent-looking message. However, once the victim clicks the file or opens the file, a virus or malware gets activated that can cause a significant level of spying on computers or identity theft. Aside from “phishing” it is also important to learn more about cyberstalking, because it can turn into a deadly exercise. It has the capability to destroy relationships or friendships, careers, selfimage and confidence. Moreover, cyberstalking can escalate into something more serious. For example, cyberstalking can easily cause serious bodily or physical harm if the perpetrator of the crime decides to literally stalk the person that he or she sees online. Merritt explicitly states that domestic-violence victims usually have a type of relationship with cyberstalking. It is therefore highly important for society to learn more about these things in order to develop appropriate policies that discourages Internet fraud, related illegal activities and unwholesome acts committed using the Internet.