IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 01, August 2018)

Cyberspace Security: An Epidemic in Identity Theft

Sudhirkumar Jagadishbhai Patel
Ph.D Scholar
Mewar University
Gangrar, Chittorgarh, Rajasthan (India)

Dr. Chandikaditya Kumawat
Professor, Computer Science Department
Mewar University
Gangrar, Chittorgarh, Rajasthan (India)

***Abstract* — Over the past few decades, the issue of cyber security has become increasingly prevalent in modern society. Because of the technological innovations that engineers have made, we now rely on computers for just about every aspect of our daily lives. However, some of these rapid improvements in technology and computer infrastructure have led to an epidemic of problems within both small and large networks. Because computers are still a modern innovation, there is a need for ongoing and rapid improvement, which explains why there are so many flaws in our security systems. This paper is an epidemic summary to consider as an introduction to the world of cyberspace, its issues and challenges.**

***Keywords* — Cyberspace, Cyber-security, Cyber-war, Cyber-criminality, Phishing.**

I. INTRODUCTION

As the National Academy of Engineering stated, there is an obvious problem within the field of cyberspace security: “Identity theft is a burgeoning problem. Viruses and other cyber-attacks plague computers small and large and disrupt commerce and communication on the Internet” [1]. Obviously, these security threats are apparent and can strike personal as well as corporate users.

Since the introduction of the consumer Internet in approximately 1988, the number of Internet users doubles every year. The Internet now allows 22% of the world's population to exchange data, chat in the forums, learn, play and shop. And by building links between them, Internet users have gradually shaped communities, then a cyberspace, which is virtual, but essential for many of them. No hierarchical structure, no pyramid, it is a network that works as we say "peer-to-peer", and that may explain its exponential development. The network is global and without borders.

The concept of cyberspace appeared in the pen of the novelist William Gibson in the 1980s, but will begin to take its political and geopolitical form only from the late 1990s. Its status remains a highly controversial issue, the answer drifting often of the nature the transmitter. Thus governments and political science theorists and international relations see cyberspace as a space subject to the same principles as the other four (air, land, sea, space), where independent actors like Wired magazine conceive cyberspace as a space without borders and totally "free".

The concept of cyberspace appeared in the pen of the novelist William Gibson in the 1980s, but will begin to take its political and geopolitical form only from the late 1990s. Its status remains a highly controversial issue, the answer drifting often of the nature the transmitter. Thus governments and political science theorists and international relations see cyberspace as a space subject to the same principles as the other four (air, land, sea, space), where independent actors like Wired magazine conceive cyberspace as a space without borders and totally "free".

Although early hackers such as Kevin Mitnick used telephone connections and first Internet connections in a roundabout way before anyone else, the first hack went back to the 1960s. Nevertheless, the massive use of cyberspace for diverted purposes remains correlated with the massive arrival of computers with an internet connection in homes in the 1990s and will eventually be exponential, the number of cyber-attacks and jobs diverted from cyberspace has continued to grow ever since.

A. Main Notions

1) Cyberspace

If the term is often approached as a synonym for the Internet, there is a whole literature specific to the more "global" concept of Cyberspace and particularly in relation to the ideals that are commonly associated with it, including the freedom of information and expression.

2) Cyber-security

Set of standards, tools, institutions and other policies associated with the regulation of the Internet and and the concept of digital trust. It primarily concerns companies that are victims of computer attacks.

3) Cyber-war

Use derived from cyberspace for offensive purposes

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 01, August 2018)

in the state domain, often through cybernetic attacks aimed at damaging or paralyzing a computer network or other structure with computer programs.

4) Cyber-criminality

Use derived from cyberspace, regrouping all criminal offenses committed against or by means of a computer system. The methods and purposes of these attacks can vary considerably depending on their author (see below) and their purpose. Thus, the recent attack against the bank of Bangladesh requires a level of technicality and expertise far beyond the simple attempt of "phishing" by email that the experienced surfer will identify immediately.

5) Deep Web and Dark Web

If many of these offenses pass through the "referenced" Internet, that is to say, accessible by search engine like Google, there is another facet of the Internet much less known to the general public and commonly called Deep Web. This immersed internet is not clearly defined or delimited and corresponds to a space infinitely more "voluminous" than the referenced web: from 15 to 500 times bigger according to the sources. As such, the Deep Web is therefore a preferred tool for many players in the illegal economy as well as for activists and private communities (see the recent appearance of "private" digital libraries on the Deep Web).

Cybercrime via the Deep Web is called "Dark Web" and is gaining increasing attention from the media, institutions and individuals. Cases have thus been widely publicized, such as the "Silk Road" website, referring to the route taken by heroin sellers from Afghanistan to Europe are offered to purchase various illegal products and services: drugs, weapons, wave jammers, bank details, computer attacks. Twice, the site was closed by the authorities and reopened by Internet users. Legal and illegal transactions are carried out in bitcoins, an electronic currency not regulated by the states.

B. Main Cause

1) Hackers and Pirates

The two terms are to be distinguished. The hacker aims, through a clever use of the Internet, to make its contribution, according to a certain ethic. The hacker is a criminal, who takes advantage of the vulnerabilities. Some US companies have learned to turn hacker capabilities to their advantage by challenging them to attack their site, with a promise of hiring if successful.

2) Governments

Governments are important players in the Internet because of their regulatory capacity. Their regulatory action influences the behavior of Internet users. The more Internet access is controlled, the more likely they are to use the Deep Web to access uncensored information. States are also actors in cyber warfare, as sponsors and targets of cyber-attacks.

3) Autonomous Collectives and Civil Society

Groups have formed on the Internet, bringing together people claiming the same cause by computer means, "hacktivists" (contraction of "hacker" and "Activist"). Groups like Anonymous and the Chaos Computer Club work to defend freedom of expression and information.

Civil society has also appropriated the cyber space to organize itself politically, especially in contexts of strict control of information and political protest.

Private companies

Private companies are also privileged targets of computer attacks. Many reasons (theft of sensitive data, blackmail) make them specific targets. They are also actors in the fight against cybercrime, the cybersecurity market experiencing strong growth.

Internet users

Internet users can be guilty and victimized in cyberspace, sometimes both. Many of them have already downloaded content illegally; many are also the victims of hacking. Often, data allowing piracy (email, password, and bank codes) are given voluntarily by the user fooled by a fake web page, which underlines the need for awareness in this sense.

II. Identity Theft

While the overall need for internet security is clear, one area that I find to be of urgent concern is the development of safety tools for identity theft. Obviously, when dealing with such a sensitive matter and trying to find a solution to these problems, it is imperative that engineers follow a strict protocol in order to keep away from underlying ethical issues. If engineers did not have any form of authority to adhere to, there would be an outbreak of controversy within just about every major engineering project. Because of this, The National Society of Professional Engineers has established specific rules within each discipline of engineering which keep controversy to a minimum. The implementation of these rules allows for an end to ethical debate and also makes every engineering project much safer. Cyberspace security is vital, because there are many hackers out there learning about the next security system; however, it is equally important that the formulation of newer and better technology is gone about in a professional and safe manner. In order to understand why these ethical issues are of great importance, we must have a firm understanding of the technology and the task that engineers face.

III. Modern Technology

Computers have played a tremendous role in the advancement of human beings and it would be a

IJDACR
International Journal Of Digital Application & Contemporary Research
International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 01, August 2018)

shame to ignore the many positive effects of computer technology. A very useful tool which has recently been implemented to increase security is the use of facial recognition and fingerprinting. This technology is referred to as biometrics. Biometrics is perhaps one of the most fascinating innovations within the computer world and is truly a landmark for future developments. There are many obvious benefits to this type of security. "The general advantage of biometrics is that it does not rely on cards or other artifacts that can be stolen or otherwise transferred from one person to another" [2]. Because biometrics have the potential to make transactions much safer, it is rapidly becoming more popular. This technology allows users to keep their personal information much more secure and it is comforting to know that such improvements are being made in the field of computer engineering. These advancements allow for a more secure form of identity authentication and diminish fraudulent charges.

"Facial scanning uses cameras and image analysis software that looks at areas of the human face that change little during the course of life and are not easily alterable, such as the upper outline of the eye sockets and the shape of the cheekbones" [2]. This type of technology makes it extremely difficult for hackers and other criminals to beat the security systems.I believe that if we could somehow use this technology to make monetary transactions over the internet more secure, it would be a major steppingstone in the advancement of computer security.

IV. Ethical Debate

Obviously, this type of technology has the potential to create many ethical debates which would be counterproductive in the eyes of the entire engineering community. Therefore, it is important for engineers to make logical decisions about whether or not a certain innovation could potentially spark controversy in their community. For example, when dealing with personal information that is sent over the internet, there cannot be any question about whether or not this type of information is secure and in the right hands. It would be naïve to think that nobody will have access to our personal information, but it is still important that the people that are given these positions are honorable and trustworthy. Personal information such as social security numbers can be as dangerous as live ammunition if put into the wrong hands.

V. Ethical Issues: A Grand Challenge

As previously stated, one of the Grand Challenges of Engineering is to implement a newer and more feasible means of cyberspace security in order to combat identity theft. It is truly a grand challenge because of the ethical significance that surrounds it. It has the potential to both positively and negatively affect our entire world and could prove disastrous if it is not handled in the right manner. Because of this, there are many ethical codes set out by The NSPE which help protect the public from dangerous and risky procedures. One code that I believe is especially important for computer engineers is to act faithfully as both an agent and a trustee. This is one of the fundamental canons of the organization and is explicitly described as a vital and necessary rule that must be followed: "Engineers shall not accept compensation, financial or otherwise, from more than one party for services on the same project, or for services pertaining to the same project, unless the circumstances are fully disclosed and agreed to by all interested parties" [3]. In simpler terms, this code of ethics simply states that engineers should not use information about a project they are working on for monetary or any other form of personal gain. This is so important because of the issue of identity theft. When given such an important role in combatting white collar crime, it is important that these people act in a professional manner and that they do not have any preconceived notions that they are entitled to do whatever they want with this information. The professional engineers working on these projects are privileged to take part in the creation of this technology and should therefore be respectful and courteous of their clients' personal information.

VI. IEEE Code of Ethics

In addition to the rules that are outlined by The NSPE, there are many other organizations set up within each discipline of engineering which have more role-specific codes of ethics. The IEEE is an organization which has created a code of for computer and electrical engineers. One of these codes that I found particularly interesting relates to the development of newer technology and is meant to avoid trademark infringement: "To seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others" [4]. This is very important because along with the development of newer technology comes money, which can cause greed. I was surprised to find a code which helps protect other engineers within a community. This code explains that it is important that we give credit to the people that create the technology which helps us. Another aspect of this code that I find to be particularly important is that engineers should allow others to critique their work. When dealing with such technical advances, this is a good way to make sure that the technology is safe and

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 01, August 2018)

beneficial to society. Engineers have to learn to accept criticism because these jobs entail cooperating with others in order to make the best product possible.

VII. Educating Identity Theft

All in all, the progress that has been made in the field of computer engineering is booming and is vital to the development of our society. An article written by Dan Gotterbarn about software engineering codes of ethics describes the importance of these rules: "If a code is sufficiently detailed it helps to educate clients and society about what can reasonably be expected from software engineers and expected from their products" [5]. These expectations can help in the development of the best technology because the engineers are set to such a high standard by everyone around them. Modern-day computer engineers are pioneers within their field and have been given a tremendous task to fulfill. Clearly, there have been many great discoveries in this field as well as a spark of interest within this discipline of engineering. Because of the many young people that are becoming more interested in computer technology, it is important that engineers continue to make this progress. It is also important that younger generations of future engineers understand the ethical issues which surround the development of newer and more advanced technology. If we can understand a Grand Challenge and understand the rules behind it, we will be able to find ways to improve it and make it a safe and useful technology.

VIII. Conclusion

Ideally, engineers will soon be able to create even more advanced forms of biometrics which will allow users to keep their personal information safe. The implementation of such devices is necessary so that sending out sensitive information over the internet is more secure. While it is important that engineers work rapidly to solve these problems, it is imperative that they follow the protocol which is outlined by The NSPE and other professional organizations. These organizations have been created for a reason, and it is vital that engineers as well as future generations of engineers understand this. In today's society, learning to balance innovation and creativity with logical and structured procedures will truly prove to be a grand challenge.

References

[1] (2010) "Secure Cyberspace." *National Academy of EngineeringGrand Challenges For Engineering.*[Online]. Available: http://www.engineeringchallenges.org/cms/8996/9142.aspx

[2] Henderson, Harry. (2007, April 20). "Biometrics."*Science Online*.[Online]. Available: http://www.fofweb.com/activelink2.asp?ItemID=WE40&SID=5&iPin=ECSRE0052&SingleRecord=True.

[3] "NSPE Code of Ethics for Engineers" http://www.nspe.org/Ethics/CodeofEthics/index.html. Accessed 24 October 2010.

[4] "IEEE Code of Ethics" http://www.ieee.org/membership_services/membership/ethics_code.html. Accessed 24 October 2010

[5] "Specifying the Standard: A software engineering code of ethics"

[6] http://portal.acm.org/wf2dnvr1 Accessed 26 October 2010