An investigation of the Issues and Solutions to Cyberspace Identity Theft and Crimes

Amos Olagunju¹, Solomon Demmessie²
Computer Science and Information Technology¹, Advanced Program in Science and Technology²
St. Cloud State University

Email: aoolagunju@stcloudstate.edu

ABSTRACT

This research investigated the problems and solutions to cyberspace identity theft. Collections of literature were reviewed to identify the issues and solutions to cyberspace identity theft. A survey was administered to a focus group of students who participated in an advanced summer scientific project, to ascertain the awareness of cyberspace identity theft by high school students.

Keywords: cyberspace identity theft, cyberspace crimes.

1. INTRODUCTION

This research reviewed a variety of literature to identify the definitions; the victims, their characteristics and theft effects; the existing laws; and technological solutions to cyberspace identity theft (CIT). High school students were surveyed to learn about their knowledge of CIT and cyberspace crimes.

1.1 Definitions and Views of CIT

There are three types of identity theft: with a “new account” identity theft, the identity thief steals information from the victim and uses the personal information of the victim to create an account for signing up; in an “existing account” identity theft, the thief steals the victim’s information for accessing their bank accounts to steal money; with a “synthetic” identity theft, the thief combines personal information with fictional information to create a new profile or account for a website [6].

The definition of identity theft differs from state to state. For example, in California, identity theft occurs when someone “willfully obtains personal identifying information of another person and uses that information for any unlawful purpose, including, obtaining or attempting to obtain, credit, goods, services, real property, or medical information without the consent of that person”. In Texas however, identity theft occurs when someone has the “intent to harm or defraud another, obtains, possesses, transfers, or uses identifying information of another person without the other person’s consent.” [8]. Unfortunately, neither of these two definitions, nor any other law in any state, differentiates between the different types of identity theft.

Identity theft also occurs when a person impersonates or captures information and uses it to steal the assets of the owner. Stealing here does not necessarily refer to tangible objects, but identity theft is committed for financial benefits or other criminal acts [9].
1.2 Victims, Effects and Characteristics of CIT

Most victims of cyberspace identity theft are corporations and people tied to corporations [4, 5, 6]. For example, on March 28, 2007, the TJX Companies Inc. announced it was a victim of a data breach that lasted one and a half years, when hackers repeatedly accessed credit and debit card information of tens of millions of customers, and stole millions of dollars [6]. Consequently, when hackers break into the unsecured computers of large corporations they can access tons of information on customers.

More money is lost each year due to corporate bankruptcy than identity theft, but CIT in rare cases, can force a company into bankruptcy [4]. Cyberspace identity theft can be expensive to avoid. Many victims of identity theft or people close to victims pay around $100 a year to frequently track Internet usage. A guaranteed CIT protection coverage plan for a business company costs around $25000 a year [4]. CIT seems to increase paranoia in everyday people and even more to large corporations.

Organizations are constantly under attack from identity thieves and should take necessary actions to help protect them and the personal information customers. A high security in organizations will help customers because identity thieves will not have access to the personal information on the millions of people [5].

Individuals who conduct businesses with organizations are frequently victims of identity theft. In today’s online world, people leave digital footprints behind them everywhere they go and shop online [1]. The novice on the Internet sometimes assumes that every website is secure from identity thieves. However, websites rarely take responsibility for identity fraud unless the case involves millions of people [1]. Identity theft is shocking and could induce fear later on the victim. For instance, a thief could use a false credible name to publish an article, or sell or buy an item [3].

The effects of identity theft are not just on devastating money lost. For example, an anonymous family, the “Smiths” was looking to purchase a house; however, they never knew they were victims of an identity fraud in which a thief borrowed thousands of dollars in their name, and ruined their credit scores [10].

1.3 CIT Laws and Court Cases

The Red Flags Rule went into effect on January 1, 2011. This rule was designed to ensure that organizations and corporations have procedures in place to protect and remedy patterns, practices, and activities that may somehow be tied to identity theft [2]. Basically, this law requires organizations to put an effort to protect customers and associates from identity theft.

The most significant court case occurred when identity theft was recognized as a crime in 1998 with the passage of the Identity Theft and Assumption Deterrence Act (ITDA). Under ITDA, “identity theft” consists of the knowingly transfer, possession, or usage of any name or number that identifies another person, with the intent of committing or aiding or abetting a crime [6].

1.4 Technological Solutions to CIT

Organizations have massive databases that hold information on thousands to millions of customers, business partners, and even employees. Identity thieves hack into the databases of large organizations and instantaneously have access to information on millions of people [7]. One way to prevent identity theft is to protect access to online transactions in business organizations. Large organizations have a responsibility to implement some security standards to deny identity thieves access to the databases of millions of credit card numbers, phone numbers, and other personal information of customers [5]. Therefore, it is imperative that enterprises invest in advanced security systems to protect computer systems with access to the cyberspace.

1.5 Scope of CIT Problem

Identity theft has been a problem since the days of paper money. However, with the invention of cyberspace and the spread of information technology, identity theft has taken more shapes and forms than we have never seen before. It affects individuals, families, and even organizations. Billions of dollars are lost each year due to identity theft in the U.S alone. Some of that money probably belongs to you, a family member, or a friend. The goals of this research were to investigate the characteristics of identity theft, to assess the knowledge of high school students about
identity theft, and to recommend solutions for overcoming identity theft.

2. METHODOLOGY

This research reviewed a homogeneous collection of literature to respond to issues associated with identity theft. The sets of related literature are clustered and critiqued to respond to each research question. A survey instrument was designed and administered to students who participated in the Scientific Discovery Program (SDP) and Advanced Program in Technology and Science (APTS) at St Cloud State University in 2012, to tap the perceptions of adolescents on the effects and solutions to cyberspace identity theft.

The survey contained questions that elicited the concerns and opinions about the Internet access and safety. The survey responses represented the awareness of high school students about Internet and email policies, and the potential dangers of identity theft in cyberspace. Unfortunately, only twenty-five students participated in this focus group survey. This makes it difficult to generalize the research findings.

The survey instrument contained three main sections. The first section categorized the survey participants based on age, gender, and familiarity with different online experiences. The second section focused on tapping the concerns of the respondents about privacy, security and threats, child protection on the Internet, e-mail safety, censorship, and impersonation and forged identity. The participants rated the topics in section two on a scale from one to five, one representing the highest level of concern, and five representing the lowest level of concern. The third section of the survey focused on tapping the opinions of high school students about the Internet safety. Each question item was rated as strongly agree, or agree, or neutral, or disagree, or strongly disagree.

The percentages, frequency distributions and graphs were generated to provide the interpretation of the survey items.

3. RESULTS AND INTERPRETATION

For the purpose of the survey results and interpretation, students refer to the 2012 summer participants in the SDP and APTS at St Cloud State University. Only twenty-five students completed the survey instruments. Thus, we only provide the descriptive and not the inferential statistics.

3.1 Student Profiles

Figure 1 displays the frequency of the students in each grade. Eight percent (8%) are in grade 9, 40% are in grade 10, 44% are in grade 11, and 8% are in grade 12. The majority of the students are in grades 11 and 12.

Figure 2 shows the number of males and females that participated in the survey. Thirty-six percent (36%) of the surveyed were males, and 64% were females. There were almost twice as many females as males.

3.2 Student Access to Email

Figure 3 displays the number of students that have an email account. Ninety-two percent (92%) of the surveyed students had an email, and only 8% did not. This shows that most of the students have an email account.

Figure 4 illuminates the number of students with different types of email accounts. Sixty percent (60%) of the students had a home email account, 8% had a work email account, 8% had a school email account, and 16% had a different kind of email account. The majority of the students had a home email account.

3.3 Student Awareness of Internet Policies

Figure 5 shows the students in schools with or without an Internet policy. Sixty-eight percent (68%) had a school email policy, 4% did not, and 28% did not know if their school had a policy. The majority of the students claimed that their schools did have an Internet policy.

Figure 6 displays the students in schools that monitor or did not monitor their email usage. Twelve percent (12%) of the students thought their schools monitor email usage, 40% did not think that their schools monitored it, and 48% did not know if their schools did or did not monitor the email usage. The majority of the students surveyed either did not know if their email usage was monitored, or thought that the school did not monitor it.

Figure 7 illustrates ways that schools monitor email usage. Out of the four students who thought they knew how their
schools monitored email usage, 50% of them thought that it was monitored through intercepting emails, 25% of them thought that their schools monitored their usage, and 25% of them thought it was made possible by filtering and blocking. Exactly half of the students thought that it was made possible by intercepting.

Figure 8 displays the amount of students who expressed opinions on the use their schools email for personal use. Sixty-eight percent (68%) said that they were allowed to do so, and 32% said that they were not. The majority of the students felt as though they were allowed to use their schools email accounts for personal use.

3.4 Student Activities on Internet

Figure 9 illuminates the students who expressed opinions on purchasing items online. Sixty percent (60%) said that they have purchased items online, and 40% said that they have not. The majority of the students have purchased things online.

3.5 Student Purchasing Concerns on Internet

Figure 10 shows the number of students who expressed opinions about placing their personal information online. Seventy-two percent (72%) claimed to be concerned when putting their personal information online, and 28% claimed to not be concerned. The majority of the students were concerned placing personal information online.

Figure 11 displays the number of students that would purchase things online if their concerns were addressed or eliminated. Sixty-four percent (64%) said they would, and 36% said they would not. The majority of the students claimed that they would purchase things online if their concerns were addressed.

3.6 Student Concerns about Internet

This section presents the results of students who expressed concerns about the Internet safety. The students rated each item on a scale of 1 to 6, with 1 indicating the highest level of concern and 6 the least level of concern. The respective percentages of the levels of indicated concerns are provided, with the first percentage representing level 1, and the last percentage representing level 6.

Figure 12 displays the number of students who expressed concerns about online privacy. The percentages are: 48%, 20%, 20%, 0%, 4%, and 8%. The majority of the students indicated at least strong concerns (level 1 or 2).

Figure 13 shows the number of students who expressed concerns about online security and threats. The percentages are: 32%, 20%, 24%, 12%, 8%, and 4%. The majority of the students indicated at least strong concerns (levels 1, 2, or 3).

Figure 14 illuminates the number of students who are concerned about child protection on the Internet. The percentages are: 8%, 16%, 20%, 16%, 28%, and 12%. The majority of the students indicated levels at least no major concerns (levels 3 to 5).

Figure 15 displays the number of students who expressed concerns about E-mail safety. The percentages are: 8%, 12%, 16%, 16%, 20%, and 28%. The majority of the students indicated at least no major concerns (levels 4 to 6).

Figure 16 shows the number of students who expressed concerns about online censorship. The percentages are: 4%, 16%, 4%, 28% 16%, and 32%. The majority of the students indicated at least no major concerns (levels 4 to 6).

Figure 17 illuminates the number of students who expressed concerns about online impersonation and forged identity. The percentages are: 8%, 12%, 16%, 12%, 24%, and 28%. The majority of the students indicated at least no major concerns (levels 5 or 6).

3.7 Student Opinions about Internet Safety

This section presents the results of students who expressed opinions on the Internet safety. The students rated each item on a scale of 1 to 5, with 1 indicating the highest level of agreement and 5 the least level of agreement. The respective percentages of the levels of indicated opinions are provided, with the first percentage representing level 1 (strongly agreed), and the last percentage representing level 5 (strongly disagreed).

Figure 18 displays the number of students who agreed or disagreed with the statement, “E-mail safety is becoming an increasingly important issue”. The percentages are:
28%, 36%, 24%, 8%, and 4%. The majority of the students at least agreed.

Figure 19 shows the number of students who agreed or disagreed with the statement, “Schools have the right to access email and Internet sites used by their students.” The percentages are: 8%, 4%, 28%, 36%, and 24%. The majority of the students at least disagreed.

Figure 20 illuminates the number of students who agreed or disagreed with the statement, “The privacy of Internet users is greatly violated.” The percentages are: 8%, 36%, 40%, 16%, and 0%. The majority of the students agreed or were neutral.

Figure 21 displays the number of students who agreed or disagreed with the statement, “To reduce the risk of liability, organizations should institute an e-mail policy and distribute it to all students.” The percentages are: 8%, 48%, 24%, 12%, and 8%. The majority of the students at least agreed.

Figure 22 shows the number of students who agreed or disagreed with the statement, “Despite safety precautions in place today, Internet and email are not safeguarded enough”. The percentages are: 12%, 56%, 20%, 8% and 4%. The majority of the students at least agreed.

Figure 23 displays the number of students who agreed or disagreed with the statement, “Schools can disclose personal information if they deem it necessary.” The percentages are: 8%, 16%, 36%, 36%, and 4%. The majority of the students were neutral or disagreed.

Figure 24 shows the number of students who agreed or disagreed with the statement, “The current school laws and regulations are sufficient for protecting information system users.” The percentages are: 4%, 12%, 48%, 32%, and 4%. The majorities of the students at least agreed or were neutral.

Figure 25 illuminates the number of students who agreed or disagreed with the statement, “The current security features such as encryption and passwords are sufficient to provide security and safety on the Internet.” The percentages are: 8%, 12%, 48%, 32%, and 0%. The majorities of the students were neutral or disagreed.

Figure 26 displays the number of students who agreed or disagreed with the statement, “E-mails are less safe than regular mails”. The percentages are: 8%, 48%, 40%, and 4%. The majority of the students at least agreed.

Figure 27 shows the number of students who agreed or disagreed with the statement, “Internet shopping is less secured than mail order. The percentages are: 12%, 20%, 44%, 20%, and 4%. The majorities of the students at least agreed or were neutral.

Figure 28 illustrates the number of students who agreed or disagreed with the statement, “I feel safe when I release my credit card information on the internet. The percentages are: 0%, 12%, 16%, 32%, and 40%. The majority of the students at least disagreed.

Figure 29 displays the number of students who agreed or disagreed with the statement, “Most emails are accessed by people other than the owners. The percentages are: 12%, 32%, 32%, 20%, and 4%. The majorities of the students at least agreed or were neutral.

Figure 30 shows the number of students who agreed or disagreed with the statement, “Only limited amount of personal information should be requested from children on the internet”. The percentages are: 36%, 36%, 16%, 12%, and 0%. The majority of the students at least agreed.

Figure 31 illuminates the number of students who agreed or disagreed with the statement, "Children should not be asked to provide information on their parents on the internet”. The percentages are: 36%, 32%, 24%, 8%, and 0%. The majority of the students at least agreed.

Figure 32 displays the number of students who agreed or disagreed with the statement, “Stalking and impersonation are common on the internet”. The percentages are: 40%, 28%, 32%, 0%, and 0%. The majority of the students at least agreed.

Figure 33 shows the number of students who agreed or disagrees with the statement, "Some e-mails do not come from the people that appear to send them.” The percentages are: 48%, 24%, 24%, 4%, and 0%. The majority of the students at least agreed.

Figure 34 displays the number of students who agreed or disagreed with the statement, “Security and privacy concerns are barriers for my shopping online”. The
percentages are: 8%, 24%, 52%, 12%, and 4%. The majorities of the students were neutral.

4. CONCLUSIONS

This research investigated the significance impacts of identity theft on individuals and enterprises. The survey results indicate that high school students recognize the effects of identity thefts on the society. Although they are ignorant of some potential dangers of cyberspace identity theft, they are aware of many of the Internet safety issues. Unfortunately, high school students are still not less susceptible to cyberspace identity theft. Consequently, high school students require ongoing training about the threats and solutions to cyberspace identity thefts.

5. REFERENCES


Figure 4 Distributions of Email Accounts

Number of Students with Different Types of Email Accounts

<table>
<thead>
<tr>
<th>Type</th>
<th>Number of Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal</td>
<td>10</td>
</tr>
<tr>
<td>Work</td>
<td>5</td>
</tr>
<tr>
<td>Personal/Work</td>
<td>5</td>
</tr>
<tr>
<td>Don't know</td>
<td>2</td>
</tr>
</tbody>
</table>

Figure 5 Frequencies of School Internet Policies

Students with or without a School Internet Policy

<table>
<thead>
<tr>
<th>Policy</th>
<th>Number of Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>20</td>
</tr>
<tr>
<td>No</td>
<td>5</td>
</tr>
<tr>
<td>Don't know</td>
<td>2</td>
</tr>
</tbody>
</table>

Figure 6 Schools Monitoring Email Usage

Students Whose School Monitors Their Email Usage

<table>
<thead>
<tr>
<th>Monitor Email Usage</th>
<th>Number of Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>15</td>
</tr>
<tr>
<td>No</td>
<td>5</td>
</tr>
<tr>
<td>Don't know</td>
<td>2</td>
</tr>
</tbody>
</table>

Figure 7 Techniques Used to Monitor Email Usage

Ways That Schools Monitor Email Usage

<table>
<thead>
<tr>
<th>Monitoring Method</th>
<th>Number of Schools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercepting</td>
<td>5</td>
</tr>
<tr>
<td>Monitoring</td>
<td>3</td>
</tr>
<tr>
<td>Filtering/Bl...</td>
<td>2</td>
</tr>
</tbody>
</table>

Figure 8 Schools Allowing Email for Personal Use

Students Allowed to Use School Email For Personal Use

<table>
<thead>
<tr>
<th>Use Email For Personal Use</th>
<th>Number of Schools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>20</td>
</tr>
<tr>
<td>No</td>
<td>10</td>
</tr>
</tbody>
</table>

Figure 9 Students Who Have Purchased Online

Students Who Have Purchased Things Online

<table>
<thead>
<tr>
<th>Purchased Online</th>
<th>Number of Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>15</td>
</tr>
<tr>
<td>No</td>
<td>5</td>
</tr>
<tr>
<td>Don't know</td>
<td>2</td>
</tr>
</tbody>
</table>
Figure 10 Concerns about Information Abuse

Number of Students Concerned About Abuse of Personal Information Online

Yes | No
---|---
15 | 5

Figure 11 Concerns about Purchasing Online

Students That Would Purchase Things Online if Their Concerns were Addressed

Yes | No
---|---
15 | 5

Figure 12 Concerns about Internet Privacy

Students Concerned About Internet Privacy on a Scale From 1 to 6, 1 Being the Most Important

1 | 2 | 3 | 4 | 5 | 6
---|---|---|---|---|---
15 | 10 | 5 | 2 | 0 | 0

Figure 13 Concerns about Online Security Threats

Students Concerned About Online Security Threats on a Scale From 1 to 6

1 | 2 | 3 | 4 | 5 | 6
---|---|---|---|---|---
8 | 6 | 4 | 2 | 0 | 0

Figure 14 Concerns about Online Child Protection

Students Concerned About Online Child Protection on a Scale from 1 to 6

1 | 2 | 3 | 4 | 5 | 6
---|---|---|---|---|---
8 | 6 | 4 | 2 | 0 | 0

Figure 15 Concerns about Email Safety

Students Concerned About E-mail Safety on a Scale From 1 to 6

1 | 2 | 3 | 4 | 5 | 6
---|---|---|---|---|---
8 | 6 | 4 | 2 | 0 | 0
Figure 16 Concerns about Online Censorship

Students Concerned About Online Censorship on a Scale From 1 to 6

Figure 17 Concerns about Online Impersonation

Students Concerned About Online Impersonation on a Scale from 1 to 6

Figure 18 Reactions of Students to Email Safety

Email Safety is an Important Issue

Figure 19 Reactions to Accessing Internet Sites

Schools Should Have the Right to Access E-mail and Internet Sites Used by Students

Figure 20 Reactions to Privacy of Internet Users

The Privacy of Internet Users is Greatly Violated

Figure 21 Responses to Email Policies

To Reduce the Risk of Liability, Organizations Should Have an E-mail Policy
Figure 27 Reactions to Internet Shopping

Internet Shopping is Less Secure Than Mail Order

Figure 28 Reactions to Online Credit Card

I Feel Safe When I Release My Credit Card Information on the Internet

Figure 29 Opinions on Others Accessing Emails

Most E-mails are Accessed by People Other Than the Owners

Figure 30 Reactions to Children - Information

Only a Limited Amount of Information Should be Requested From Children on the Internet

Figure 31 Responses to Children Information

Children Should Not be Asked to Provide Information on Their Parents Online
Figure 32 Reactions to Stalking and Impersonation

Stalking and Impersonation are Common on the Internet

Figure 33 Responses to Emails from Non Owners

Some E-mails Do Not Come From the People that Appear to Send them

Figure 34 Reactions to Online Shopping Security

Security and Privacy Concerns are Barriers for My Online Shopping