Online Scams: On the Rise or Decline?

A Case Study

Group 9

4/25/2012

Table of Contents

1. Introduction

The Internet is an essential aspect of today's world; almost everything is related with it. It makes our life easy through lots of features such as email, information, services, e-commerce, and communities. Millions of peoples' sources of income are now dependent on the Internet. Earning money from home, getting a degree online, and seeking a job are some known advantages of the Web. However, it also makes everything simple for crooks to conduct online scams. Thieves can now easily do their activities and take advantage of people on the Internet. Fake check scams, auctions, money offer, lotteries, advance fee loans, prizes, credit repair, travel, fake scholarships, and phishing are some well-known methods of online scams. It can occur in chat rooms, message boards, emails or Web sites. According to statistics, "the total loss for online scam in 2005 was $13,863,003" (National Consumers League[3], 2012) and 24 percent of these are initiated by email.

Online scam is one of the greatest concerns of our current technology. It is very important for us to study this subject matter as this is related to social, legal, or ethical aspects of information technology. Although online theft might be increasing gradually, we shouldn't be kept away from the benefit of using the Internet. Instead, we should take appropriate steps against online scams such as doing business with companies that we know and trust, checking all bills and invoices carefully, protecting our financial and account information, and educating employees about avoiding scams.

Online scams are increasing day by day due to the number of gadgets and apps growing at a faster rate. Eventually, all of our activities and services are going to be online based. Our computers and cell phones are almost continuously connected online so it becomes simpler for criminals to hack into our systems. Although most people and organizations use software such as virus guards and firewalls to block these malicious attacks, hackers are discovering different means to continue their actions. In the future, online scams will become more dangerous when our daily life activities is even more computerized like automated fleets of cars communicating with each other to drive safely on highways. We have already seen some hackers who think misdirecting airplane pilots is a worthy exploit.

2. The Controversy and Overview of Different Sides

As we can see today, criminals employ many ways to make money over the cyberspace by scamming people. It is a serious issue to know whether online scam is on rise or decline because we might be the next victim and also to have the comfort of knowing that we have a safe cyberspace. You might have heard from some of your friends or have read stories about people getting scammed which led you to the notion that online scamming is on the rise. It is, in fact, relatively easy for scammers to get personal and sensitive information from potential victims due to certain factors. One of them is the target's lack of

knowledge to distinguish a scam from legitimate information. Another is the creative ways criminals employ to trick their victims into divulging personal information to seemingly trustworthy Web sites.

According to www.fraud.org, there are many criminals sellers on the internet, and "it's sometimes hard to tell the difference between reputable online sellers and criminals who use the Internet to rob people." (National Consumers League[2], 2012). A good example of this is about a 14-year-old boy named Akin from Lagos who made millions of dollars online by using fake credit cards to buy stuff online. He had the items shipped to Europe (to avoid suspicion), where he had friends ship them to Lagos and sell on the black market (Lawal, 2006). This gives us an idea that online scammers are maybe younger than what we thought; that they can come from overseas; and that their numbers are on the rise.

On the other hand, governments across the globe try their best to prevent online scams by creating regulations and passing laws. Some of these laws impose upon online retailers to pass certain requirements before they can conduct business online, or conduct appropriate punishments on scammers found guilty. (Punishments could have a deterrent effect on individuals who intend to be scammers.) For example, the Congress passed the Computer Fraud and Abuse Act (CFAA) in 1986. This law outlaws hacking activities which includes: DoS, malware, unauthorized access, fraud, impairing governments' operations, and public utilities (Liu, 2012). Not to mention the private sector's moves against online scamming, actions such as this discourage the act which potentially decreases cybercrime occurrences.

3. Individual Parts

3.1. (by Md Alam) Prevention of the Current Technologies from Online Scams

3.1.1. Choosing a Side

The internet radically changed our world and our current generation immeasurably depends on it. We cannot aspect better services without having benefit from it. Almost everything including business, education, medical technology, traveling, and communication gradually became online based. Meanwhile, crooks also distinguish the possible of cyberspace. Already many of us are victims or attempted victims of internet frauds. In the past few years many businesses and consumers lost billions of dollars in the causes of online scams. Online scams turned into one of the serious issues in our current technologies. Compared to the previous statistics of online frauds and the current increases of online technologies, I will rather say our new generations and programmers able to protect ourselves and learned how to recognize the danger signs of frauds. In that sense I believe that online scams have declined in our current technologies.

3.1.2. Arguments and Analysis

Our modern generation put more attention in online scams and extremely serious to stop and prevent such kind of cheats. Many web sites including www.fraud.org help us protect ourselves by providing sort of features such as Internet Fraud Tips, Scams against Business, Online Complaint Form and the statistics and ratios of internet frauds (National Consumers League[2], 2012). NCL's Fraud Center (www.nclnet.org) tracks telemarketing and latest internet frauds and helps consumers to avoid those scams. The well known web site like www.usa.gov provides us information about online scams and allows us report internet frauds (US Government, 2012). The National Internet Fraud Watch Information Center also allows us to report any kind of online frauds and scams so that law agencies can shut the fraudulent operations down. This organization provides us a sort of some suspicious sectors and tips of online scams such as Business Opportunities, Credit Card Loss Protection, Medicare Rx Drug Coverage, Work-at-Home, Credit Repair, Money Offers, Phishing, and so on. They also provide some general information for new internet users and new business companies to avoid possible scams such as Fax Fraud, Loan Scams, and Advertising Materials etc.

Many of our financial corresponding and transactions now became online basis. Instead of going to bank now people like to use net to pay their bills, deposit checks, transfer money, check account balances, and so on. Many of us now order things online or use online auctions instead of going to the actual shops or places. Therefore, it becomes easier for thieves to still identification such as social security number, date of birth, and bank information of an individual over the net. According to the statistic the total loss of online scams in 2005 was $13,863,000 whereas 72% of this was only for fraud auctions and online shopping (National Consumers League[2], 2012). Many organizations are now focusing to protect these kinds of frauds and taking appropriate steps to prevent these frauds. Compared to the earliest years, online crimes now turn into difficult. People became more educated to protect themselves from online crimes. Some government organizations such as National Cyber Awareness Month and NCL are working to educate consumers about the most frequent scams and commonly popping up online, often disguised as legitimate offers, meant to trick victims and steal their money (National Consumers League[1], 2012).

Gradually governments passed laws that specifically addressed computer crimes. State and federal laws are now providing strong penalties including prison sentences and fines. "Congress passed the main federal computer crime law, the Computer Fraud and Abuse Act (CFAA), in 1986. Prosecutors use more than a dozen other federal laws to prosecute people for crimes related to computer and telecommunications systems." (Baase, 2008). FBI and many law enforcement agencies are constantly working to prevent online crimes and catch hackers. Moreover, agents and security professionals are using undercover to catch hackers. They read hackers newsletters

and participate in their discussions through chat rooms and some other sources. They also provide some web sites that are attractive to hackers so that they can study the activity of hackers.

3.1.3. Relation to the Course Subject

So far we have noticed how internet and many other online features are deeply related with our daily life, and how online thieves are taking advantages of these, and lastly how our government and the law enforcement agencies are taking proper actions to stop and discontinue these kinds of crimes. All these issues mentioned above are in our course materials that we have already discussed in our class. A number or chapters of our book such as Privacy, Intellectual property, Crime, and Evaluating and controlling technology have adequate information which are connected with this topic. Specifically in chapter 5 (Crime) of our book, we have studied how hackers do their activities, what might happens in the future, the law of catching and punishing hackers, and the security which are pretty much related with this topic. Ultimately I will say, this topic relates to the social, legal, or ethical aspects of computer or information technology.

3.1.4. Conclusion

Considering all issues mentioned above, we can realize that online scams have declined instead of increasing. Our intellectual programmers and engineers are able to handle this difficulty. The government laws, agencies, and FBI took strong actions to prevent online scams. Many young hackers receive probation, community service, and fines and now most of them have matured and looking for responsible careers. No one can bring successes individually within a day but together we can change our world for the better services and technologies without scams and make a better future for our oncoming generations.

3.2. (by Zhuhe Chen) Online Retails Scam Has a Vertical Increase Rate

3.2.1. Choosing a Side

Since the number of internet visitors are getting radically increase, the crooks also see this is a good chance for investment. They setup fake website, and send out email to wait for the victim. The things that they want are not just money, and include personal information as well. Although there are many governments try to prevent online scam in order to keep us in a safe cyberspace, the number of online scam is still in raise. I do believe this because there is lard to catch the scammers and victims were lacked of knowledge about that.

3.2.2. Arguments and Analysis

You might hear some of your friends got online scam because they went into a strange website and make a purchase. In March 9, 2010, JSOnline (Ferral, 2010) reported on a widespread Craigslist scam that steals many victims' eBay login and the money in their PayPal. In those cases, the scammers post fake products for sale on Craigslist. When a buyer interested on the items, the scammers will ask the buyer to make the transaction on eBay. The scammer then sends the buyer a fake eBay website that steals the login information. If you are lacked of knowledge about this, you might be next victim. On the other hand, many governments try their best to prevent online scam by laws. These laws could be asking online retails to pass the requirement s before they start the business online, or punished the scammers in the governance range. Unfortunately, there are not every country has those laws and don't put enough budget to enforce the laws in the world. Thus, it the scammer in these countries still have the opportunity to scam other people without care about the law in over sea. In addition, it's hard to figure out who the scammer is. They are smart than we thought because they use public network submit the information online as such public Wi-Fi and computers in internet café. If there require shipment during the scamming, they will use an anonymous place as the middle transportation point as the same in Yahoo! Millionaires (Lawal, 2006). Furthermore, it's hard to trace the scammers by IP address and physical address. Although they find out the IP address or the physical address, it's still hard to enforce the law if the scammer lives over sea. This could let the scammers feel that the law doesn't anything to them. Therefore, the number of scammers keeps growing in these areas. According to Consumer Fraud Reporting.org, IC3 website received 275,284 complaint submissions in 2008, and it was 33.1% increase compare to 2007. Among of the cases, 32.9% are non-delivered merchandise and 25.5% are internet auction fraud. As we can see, most of the online scam cases are related to online retails.

3.2.3. Relation to the Course Subject

As we discuss above, online scam affect out daily life in the cyberspace. It makes the cyberspace unsafe by stealing others banking, other payment accounts and personal identities information. It also causes the governments have to try their best to protect us from online scam. Based on what we learned from this class, online scam is unethical and is a kind of crime. The scammers are mainly use theft techniques such as phishing, pharming and online resumes and job hunting sites may reveal. In additional, they also violate international agreement. Moreover, online scam also relates the chapter Privacy because the scammers don't have authentication and accessed victims' accounts or use personal information.

3.2.4. Conclusion

Based on the issues that discuss above, online scams is in raise since the laws are not that efficiency to prevent all the scammers around the world, and the scammers are hard to catch. Therefore, this caused there are more new scammers coming than old scammers get out. In addition, victims are lacked of knowledge to keep them away from online scam is one of the factors that attract more scammers join into their family. Hopefully, there will be an efficiency solution to prevent online scam in the future.

3.3. (by Dinia Gepte) Old and New Technology Aftermath

The Internet has gone a long way from its initial conception back in the 1960's as a mean to share information in military and scientific fields. It now globally connects a multitude of computers to give, share, and provide all kinds of information or service. It comes to no surprise that villains will arise to take advantage of this concept of "sharing information;" villains who we know as online scammers.

3.3.1. Choosing a Side

It was the year 2004 when a surge in the number of reports on Internet fraud was first seen (about a decade after the establishment of companies like Amazon, eBay, Yahoo; five years after high-speed Internet was made available to the public; and the year social-networking giant Facebook was launched). Since then it has considerably stayed the same until another surge was seen half a decade later in 2009. And although the most recent 2010 report of Internet Crime Complaint Center (IC3) shows that there has been a small drop in the number of cases (Internet Crime Complaint Center, 2010), after careful analysis, I have reasons to believe that it's not going down any time soon.

3.3.2. Arguments and Analysis

"A prepared statement by the FTC to the U.S. House of Representatives March 30, 2006 said identity theft victimizes nearly 10 million Americans, with costs to businesses and consumers of almost $53 billion in 2003, a 79% increase over 2002." (Dinev, 2006).

At some point, almost a decade ago, identity theft became a major public concern that it alerted higher authorities to take serious action to protect the public from this cyber attack. In response, the FBI collaborated with affected businesses, while the House of Representatives passed two bills in 2004 – Securely Protect Yourself Against Cyber Trespass (SPY Act) and Internet Spyware Prevention (I-SPY Act) – which listed phishing as a scam activity (Dinev,

2006). The private industry also boarded the bandwagon. The Anti-Phishing Working Group was formed in 2003 – the year when a reported 73% of email traffic constituted spam (or 1 in every 1.4 emails) (Furnell, 2005). The group created and maintains a website that aims to eliminate phishing and email spoofing by helping victims and raising public awareness on latest online scams including tips to fight against them. A group by e-commerce providers called Coalition on Online Identity Theft was formed on the same year sharing the same ideals (Dinev, 2006). Technology companies chipped in by selling security tools (anti-virus software), improving their products (email spam filter, firewall), or upgrading their networks (DNS server robustness and security).

With the number of key players working together to protect the public in the cyberspace, it wouldn't be wrong to assume that Internet fraud will finally be suppressed, but neither it is right. These virtual attacks are created by people; people who, just like you and me, learn from their past mistakes and improve on them. These websites that seek to educate us against online scams also attract the perpetrators themselves. They aren't foolish enough to stick to a scam that has been completely exposed; they move on to create new ones.

What used to be scams made through email, Instant Messaging, or phishing sites have made their way to new technologies and different platforms as well. This decade saw technology grow exponentially almost overnight: record-breaking sales of gadgets like smartphones, eReaders, and tablets are reported every day; the rate of changing our mobile phones as soon as the new one arrives has achieved new heights; and how the laptop you just bought six months ago is now outdated because a better, faster system has been released is simply mind-blowing. All of these have lead to new Internet fraud cases and how they take advantage of the ever-growing population who use these devices. It didn't help either when applications (apps) and digital books (eBooks) were introduced to smartphones and tablets/eReaders, respectively. Collection of credit card info became the norm to make these purchases that it is not impossible to see why scammers would exploit this means of transaction.

"A billion thanks. 25 times over." (Lawler, 2012). This is Apple's way of announcing its 25th billion download in its immensely popular App Store on March 2012. Reaching this milestone in just four years is a hard cold fact that there is no way of stopping consumers from buying digital media. Of course if I was one of the bad guys I would take this opportunity to create an app to, say, collect sensitive information, unbeknownst to the user who downloads my app. And this is exactly what they did. On December 2011, Google removed 27 apps from their Android Marketplace (now Google Play) due to a wave of attacks by a malware called RuFraud "which tricks users into agreeing to SMS charges by mimicking well-known apps such as *Angry*

Birds and *Cut the Rope*." (Fu, 2011). As a continued effort to fight against fraudulent and malicious apps in their Android Marketplace, Google announced Bouncer on February 2012, a service that will eliminate such apps (Albanesius, 2012). Despite this, two months later, an independent research by software security giant Symantec revealed results of detecting 29 malware-ridden apps from a sample of size 96 (Gupta, 2012).

3.3.3. Relation to the Course Subject

This topic is a way to raise public awareness about Internet fraud, just as how the topic on Crime in the course subject talked about various methods employed by scammers (e.g. phishing, pharming, spoofing) and how we can protect ourselves against them. On both accounts, we are informed of how the public and private sector are taking actions and how we, the public, can help their cause. As students who will be part of the computer and information technology industry, it is important for us to be aware of these things to help others who will seek professional advice, in accordance to professional ethics.

3.3.4. Conclusion

Technology expansion in the future will inevitably bring with it new kinds of cybercrime. There *are* people who will fall into victims under these new methods no matter how prepared they are. Coming from Google Bouncer's example, among many other things, even with increasing technology and practices against Internet fraud, scammers will always be one-step ahead. It is a game of cat-and-mouse where, unfortunately, there aren't enough cats to catch the mice. So, ultimately, the rise or decline of such cases lies in the hands of the smart consumer.

3.4. (by William Polenz) Enforcement, Education, & Technology

3.4.1. Choosing a Side

In recent years, we have seen a massive technological boom. The world has become increasingly inter-connected through the Internet. With increasing technology and reliance on that technology, crooks have found more ways to swindle people out of both their property and valuable personal information. There have been countless stories of spam, advance-fee fraud, stolen identity, various hacking attempts (both successful and unsuccessful) on both the government and specific citizens, and many other types of criminal cyber-activity that leaves somebody cheated. In recent years, though, there has been increased awareness and protection against such online scams, partly due to a variety of factors including: the notorious nature of

some of the scams, recent legislation on Internet scams, education on safe usage of the Internet, and efforts by e-mail providers & others to help avoid scams via the use of technology.

3.4.2. Arguments and Analysis

According to an article in the Journal of Criminal Justice, "fraud existed since the origin of recorded history, with legislation regarding fraud dating back to fourth century B.C. in ancient Greece." (Burns, Whitworth, Thompson, 2004) Since fraud is not something new, it seems that Internet fraud is simply a new avenue for fraud to take place. In this light, it seems at least part of the burden of online scams is on the ability of law enforcement and the legal system to "keep pace" with the various schemes cyber-criminals have concocted & continue to fabricate. In the US there has been plenty of legislation written to provide retribution when fraud has been committed and the perpetrators caught, but the trouble with online scams rests with the ease at which a criminal may take advantage of you and then disappear without a trace. At least 2 such bills are "…passed in 2004 by the House of Representatives—the Securely Protect Yourself Against Cyber Trespass, or SPY, Act (HR 2929) and the Internet Spyware Prevention, or I-SPY, Act (HR 4661)… " (Dinev, 2006) each of which provide some protection against cyber criminals. One might argue that the prevalence of online scams must decrease as there is an increase in the recoil expected from law enforcement if a scammer is caught.

Today, we have entire organizations and websites dedicated to helping deter fraud on the Internet. One such website is www.antiphishing.org, which provides resources to help better educate citizens on Internet fraud. There is even information on recent viruses being spread via e-mail on the home page. A list of other organizations dedicated to prevent online scams may be found via www.antiphishing.org (APWG, 2012). Many of these organizations have made a commitment to helping deter online scams. It is not likely that all of these organizations had existed a decade ago, which implies a trend towards greater education about online scams. One might argue that education is a significant factor in determining the prevalence of online scams, as a person will probably not fall for a confidence trick if they are aware of such tricks. According to an article on www.acm.org, "In 2003, Amazon.com, eBay, McAfee Security, Microsoft, Verisign, Visa, and other online retailers formed the Coalition on Online Identity Theft, aiming to raise awareness and educate the public about the growing threat of Web spoofing and how to defend against it." (Dinev, 2006). That was 9 years ago that more than 7 major online retailers recognized the significance of Web spoofing (creating a fake website with the intent to steal information; typically a fake website will mimic a legitimate site, for example an online

banking website) and contributed to helping stop it. As the years pass and people become more educated, online scammers will find it only more difficult to con some gullible web user.

A small note in an article released by the FDIC in 2004 mentions that, "Early spoofing was partly facilitated by a flaw in Microsoft's Internet Explorer program … The flaw has since been patched." (Federal Deposit Insurance Corporation, 2004). This is another example in which, years ago, large corporations had already begun to recognize the importance of online scams and made efforts to help prevent them. A more subtle point is that the technology used to perpetrate scams is being improved to help correct such flaws. It may be argued that this could only help slow down the rate at which (successful) online scams are conducted. Many e-mail providers today provide "junk" folders and filters which help remove suspicious e-mails before users even have a chance to see them.

3.4.3. Relation to the Course Subject

Above we have outlined three factors that will only increase with time and help reduce the rate at which online scams are committed. The first is the capacity for government and law enforcement to catch and prosecute online criminals; the second is the education of possible victims of online scams; and the third is smarter technology that helps prevent online scams from being possible in the first place. All of this ties in to the course material we have discussed in class for we have covered legislation & law enforcement governing the Internet (the first factor mentioned above); education of the public as a principle mentioned in the ACM SE Code for ethical professional conduct (the second factor); and the discussion of regulatory approaches to ensuring smarter technology that will prevent scams, such as spam filters & "junk" folders (the third factor).

3.4.4. Conclusion

The above arguments give some evidence that the prevalence of online scams may be dropping as effective legislation against online scams increases, education about scams increases, and technology that prevents scams increases. It is important to note that the above arguments are, by nature, speculation on what the future may hold, and that is yet to be seen.

4. Summary

The previous sections of this paper discussed arguments (and then analyzed those arguments) on the question of whether the prevalence of online scams will increase or decrease in the future. This is a particularly important question, as the answer has dire consequences of large magnitude. To give you an

idea of the magnitude we are talking about, 6 years ago the Federal Trade Commission had reported that "… identity theft victimizes nearly 10 million Americans, with costs to businesses and consumers of almost $53 billion in 2003…" (Dinev, 2006). Online scams cause damage on the order of billions of dollars.

Surely you have been convinced in an earlier section of this paper that not only is this question important for the future, but it is also controversial as there is no predicting the future. The paper you have just read begins to address and analyze some arguments for the rise of online scams and some arguments for the decline of online scams. Some of the arguments for the rise of online scams include: the idea that the Internet is connecting more people which scales with possible criminals and victims; the idea that some under-developed countries now connected to the Internet do not have adequate means to regulate or even begin to address online scams originating there; and the idea that advanced crime syndicates with internal specialization are replacing the lone-hacker of decades past. Some of the arguments for the decline of online scams include: greater education and "spreading the word" through various organizations will empower users to avoid scams; better preparation on the side of law enforcement & prosecution will deter would-be scammers; and improved technology will help stop scams before a would-be victim has the slightest hint of a scam in the making.

The arguments above are not all that may be considered, but just from what has been written it is clear that it remains debatable whether online scams will wreak havoc increasingly so in the future or mass education of online users will mitigate online scam attempts. What happens in the future is yet to be seen.

Bibliography

Albanesius, Chloe. “Google ‘Bouncer’ Now Scanning Android Market for Malware.” *PC Magazine*, February 2, 2012. http://www.pcmag.com/article2/0,2817,2399778,00.asp, accessed April 2012.

APWG, “APWG: Resources.” http://www.antiphishing.org/resources.html#antifraud, accessed April 2012.

Baase, Sara. *A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet*. Upper Saddle River, NJ: Pearson Education, Inc., 2008.

Burns, Ronald G.; Whitworth, Keith H.; Thompson, Carol Y. “Assessing Law Enforcement Preparedness to Address Internet Fraud.” *Journal of Criminal Justice* 32, no. 5 (2004): 477-493. SciVerse, accessed April 2012.

Consumer Fraud Reporting. “Internet Fraud, Scam and Crime Statistics – 2009.” http://www.consumerfraudreporting.org/internet_scam_statistics.htm, accessed April 2012.

Dinev, Tamara. “Why Spoofing is Serious Internet Fraud.” *Communications of the ACM* 49, no. 10 (2006): 77–82. ACM Digital Library via Google Scholar, accessed April 2012.

Federal Deposit Insurance Corporation, *Putting an End to Account-Hijacking Identity Theft* (PDF File), downloaded from http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf, accessed April 2012.

Ferral, Katelyn. “Phishing scam uses Craigslist to lure users to fake eBay sites.” *JSOnline*, March 9, 2010. http://www.jsonline.com/business/87178692.html, accessed April 2012.

Fu, Eddie. “Google removes 27 apps from Android Market in response to RuFraud malware threat.” TheVerge, December 14, 2011. http://www.theverge.com/2011/12/14/2635274/google-malware-apps-android-market-rufraud, accessed April 2012.

Furnell, Steven. “Internet Threats to End-Users: Hunting Easy Prey.” *Network Security* 2005, no. 7 (2005): 5–9. SciVerse, accessed April 2012.

Gupta, Rahul. “Symantec identifies 29 malware apps on Google Play.” CNN-IBN, April 23, 2012, http://ibnlive.in.com/news/symantec-identifies-malware-apps-on-google-play/251279-11.html, accessed April 2012.

Internet Crime Complaint Center. 2010 Internet Crime Report. http://www.ic3.gov/media/annualreport/2010_ic3report.pdf, accessed April 2012.

Lawal, Leonard. “Online Scams Create “Yahoo! Millionaires.” *Fortune*, June 1, 2006. http://money.cnn.com/magazines/fortune/fortune_archive/2006/05/29/8378124/, accessed April 2012.

Lawler, Richard. “Apple crosses 25 billion App Store downloads, thanks to all the little people (updated).” Engadget, March 3, 2012. http://www.engadget.com/2012/03/03/apple-app-store-25-billion/, accessed April 2012.

Liu, Yanni Ellen. “Computer Crime.” PowerPoint presentation, March 26, 2012, Stony Brook University, Stony Brook, NY.

[1]National Consumers League. “Celebrate National Security Month.” http://www.nclnet.org/technology/9-safe-computing/577-national-cyber-security-month, accessed April 2012.

[2]---. “Internet Fraud Watch: Includes Statistics on Internet Fraud.” http://www.fraud.org/internet/intinfo.htm, accessed April 2012.

[3]---, *Internet Scams Fraud Trends January-December 2005* (PDF file), downloaded from http://www.fraud.org/2005_Internet_Fraud_Report.pdf, accessed April 2012.

US Government. “Internet Fraud Information.” http://www.usa.gov/Citizen/Topics/Internet-Fraud.shtml, accessed April 2012.