Computer crime research proposal

We have to be ready for all the new ideas the tech savvy individuals are coming up with to assume ones identity. There are so many that the public cannot be warned about them all therefore schooling yourself on the security measures to take will save you the hassle In end. “ Internet Crime Trends: The Latest Report” I chose this article because It Is good to be aware of the trends that the computer criminals implement. Based on the ISRC, or the Internet Crime Report which dates Complaint Center, had were non-delivery of payment or merchandise, impersonating scams, and identity theft.

Most of the complaints came from United States residents, mostly male, between the ages of 40 and 59. Most of the complaints come from California, Texas, New York, and Florida. Those are the states that are heavily impacted because they are heavily populated. Computer criminals are far from fools. Being able to master the art of theft online is not easy. They target the cities that are fast-paced, that way they will not realize a crime is being committed until well into the process. The ICC received approximately 300, 000 complaints a year roughly 25, 000 per month.

Half of the reported complaints were of some form of financial joss. However, many internet crimes go unreported. Citizens are not aware that even if they do not fall into the trap and become a victim of a computer crime, the fact that they were contacted at all should be reported as well. According to the NCSC, or National Computer Security Survey, there are three types of cybercafé. There are the cyber-attacks, cyber-theft, and cyber-security incidents. The cyber-attacks are when the computer system in general is the target. Viruses and worms are the culprit in cyber-attacks.

Cyber-theft is when a computer is used to receive any type of uncial gain or other things of value, embezzlement and fraud are types of cyber- theft Just to name a few. Cyber-security incidents normally affect businesses. Span. Fare, Edward, Hacking and Pushing are common incidents that can happen in a business establishment. However, this is where our security needs to be in its best shape. In 2005, a study of over 7000 companies reported that 67% detected at least one cybercafé, almost 60% detected one or more types of cyber-attack, 11% detected cyber theft and 24% detected other computer security incidents (NCSC, 2005).

Many of the companies didn’t even report the crimes but the ones that were reported sustained monetary loss of $10, 000 or more. This data revealed to me that some cyber-crimes go unnoticed because they are not reported. Business companies and individual citizens alike have been victim to a potential cyber-crime whether you are aware or not. Many people do not report mainly because nothing was stolen. It takes for something to leave our possession before we react. On the contrary, with crimes like Cyber-Attacks, Cyber-Theft, and Cyber-security breaches acting on something small can save you a lot of disappointment in the end.

The fact that the trends are adapting rapidly daily does not mean that the older techniques are not still lurking. If you have received mail, physically or electronically, asking for money, claiming to be someone that needs money, or telling you how to make money it’s usually a scam. “ Cyber-Crime Taking on Sinister Forms” Nowadays, the criminals who attack via the computer are growing rapidly. Authorities feel that 2012 will be a big year for cyber criminals. Especially the scams, there have literally been hundreds of emails

sent out asking one to send money, or to cash a check then wire it somewhere else.

Often scampers assume the identity of major companies and corporation’s telling you that you can become a member of their team if you send money from one place to another. Citizens should report any suspicious activity. Older men are considered a high risk target. Unlike women, most men are not computer savvy and may fall for a scam faster than a woman would. Many scampers are unemployed and are looking to make easy money. However, we cannot to stalk and harass individuals. Usually the sender remains anonymous and their main goal is to gain access to the identity of an individual.

Based on an electronic monitoring study in 2006, 83% reported that they received an email from a stalker, 35% received an instant message. More than 3 million people, both male and female, over the age of 18 had been stalked at least once. Now of course, stalking in the physical is completely different from cyber stalking. In this sense, stalking is defined as conduct that would cause a person to feel fear. Studies show that electronic monitoring was used to stalk 1 in 13 victims. Video or digital cameras we used to spy on individuals that never knew they were being watched.

Of the 3 million people surveyed over 250, 000 sustained injuries in stalking attacks (Sodbuster & Ward, 2010). These specific attacks escalated from cyber-stalking to physical stalking, however, it everything originated online. Out of the initial survey, over 35, 000 were raped or sexually assaulted, over 50, 000 were seriously injured, and over 270, 000 individuals suffered minor

injuries (Sodbuster & Ward, 2010). This information was shocking. One never knew you could be stalked online. However, if at any point you felt any type of fear whilst online that is considered cyber-stalking.

Another fact that shocked me was that the offenders were between the ages of 18 and 29, at the same time, the victims were between 21 and 39. One would think the offenders would be older and the victims young but sadly this is not the case. “ Convenience vs.. Security When convenience versus security is compared one is aware that when you have one you have less of another. For example, shopping from home, everyone loves it, however, what if the site is not secure. Now without knowledge, your online shopping has put you at an extreme risk. Once information is entered online it’s there forever.

It can never be deleted it or retrieved. Think of all the convenience technology has blessed us with. Microwaves, no more waiting to cook on the stove; Cell phones, the ability to send and receive photos, emails, without being in front of the computer; Fax Machines, send and receive important document without waiting for the mail. Computers have made things so easy for us, but at whose expense? Us, we are the expense. Cell phones are convenient but what if a photo is sent to the wrong person, what that individual can do with a photo has endless possibilities.

What if your fax test intercepted, by someone who has no business knowing what was faxed? No one is completely sure when it happens and the victim is the only one left wondering why. Valuable information gets stolen every day at the hands of computer criminals and we are allowing them. It’s odd

that we use our computers so often and we are not schooling ourselves adequately. “ The NCAA: Combining Forces to Fight Cyber Crime” Created in 1997, by the FBI, the National Cyber-Forensics & Training Alliance (NCAA) was designed to share information that can stop emerging cyber threats and mitigate existing ones.

Assigned to the NCAA is a unit known as the Cyber Initiative them then NCAA can do their Jobs effectively. It is often used as an early warning system. Agent Eric Storm, who leads the CIRRI said, “ cyber-crime has changed so much since those early days of spamming, and the threat continues to evolve globally, which is why the Nectar’s work is so critical to both business and law enforcement”. Along with the Computer Emergency Response Team (CERT.), and the Bi’s Internet Crime Complaint Center (ICC) the FBI was able to attacked major cyber organizations.

Spam used to be their biggest problem. However, as technology regresses the now defend citizens against malicious computer viruses, stock manipulation schemes, telecommunication scams, and other financial frauds perpetrated by organized crime groups who cause billions of dollars in losses to companies and consumers. The CERT. focuses on research and education to help software and systems acquirers, managers, developers, and operators address security and survivability throughout the development and acquisition life cycles.

The team has created methods and solutions that can be integrated into existing practices. When security is built into software from the ground up, software is more assistant to attacks. And the ICC is Internet Crime

Complaint Center; this is where all complaints regarding any internet crimes go. They work closely with the FBI, they use the information they recover as means to help protect us via the web. The FBI is aware that no one organization can succeed by itself. Together these organizations can stop or at least tame cyber-crime.

They have done such a good Job already that the FBI is recognized as one of the worldwide leaders in the fight against cyber- crime. RESEARCH DESIGN: Using a non-experimental design and longitudinal studies I will be showing a impel increase of how hacking has increased over time. From the beginning when all that could be hacked are databases at major companies to how it has adapted and evolved to Pads, tablets and smart phones. The rise in technology will show a decrease in security.

Mainly because of how fast technology is adapting. I will also include a time series design. This is an “ over-time” proposal mainly because computers are advancing every day and each day something new is happening. SAMPLING: I would use is the multistage cluster sampling design and stratified design. I’m sure it is a large number of people that have been attacked, something like a population and as discussed in class this would be the best type of sampling to use when dealing with larger quantities.

The surveys will let them know they were not at fault but it will help them realize what they can do so it won’t happen again. Secondary data will be useful to me because this is information that has already been collected. I can compare that to the data I currently have and see the differences between what has happened and what is going to happen. The data that I

would view would help me help the victims that have been or was attempted to be a victim of identity theft. Lastly, the data collection technique that will benefit me is field research.

At first I thought this would not be a good method to implement for my studies but with field research you can understand deeper and be able to back your information up with facts because you saw what happened to the victim. When you take your notes you observe what you think you saw, what you know you saw and the interpretation of what you saw. Best appropriate when measuring behavior and with field research you get that. I would use the field research to see the aftermath of identity theft. How it changes the lives of the people affected.

Based on my research I some of my questions are deemed personal. However, identity theft is personal crime. I would ensure that the information is safe with me. It will never be leaked to cause personal harm. Any information that is obtained will be used solely to help not hurt. Many people become a victim of identity and theft and they do not know, based on the information that I am told I would use that to help other citizens from being a victim like watching the signs that the people before them ignored. And I would help them implement the methods to help keep them protected.