INTERNET SAFETY: HOW TO PROTECT YOURSELF FROM ONLINE RISKS

Senior Exhibition of Mastery

Emily Cavu Carson

17 April 2009

Introduction

According to a study by the Pew Internet & American Life Prodject, ninety-three percent of teenagers use the Internet, and sixty-one percent of them go online at least once a day (Makenna). Other studies have shown that Internet users, on average, spend between two and three hours on the Internet each day (Holmes). Specific results indicate that fifty-seven percent of this time on the Internet is devoted toward either email or instant messaging (McGann). Because accessing the Internet today is becoming easier, through cell phones or laptops, use of the Internet is rapidly becoming more and more frequent. Due to this growing use of the Internet and the new capabilities of web 2.0, users should be more cautious and knowledgeable about the world they are entering. To what extent does the use of web 2.0 present short or long term risks to online users? Internet users of all ages should be more aware of five major online dangers: stalking and predators, identity theft, lingering information, phishing, and cyber bullying.

The history of the computer begins in 1936 with the first freely programmable computer, the Z1 Computer, invented by Konrad Zuse. The timeline continues with the original Internet, the Arpanet, in 1969 (Bellis). Consumers were first able to purchase a computer for their homes in 1974 (Bellis). Since the release of computers into the consumer world, the number of homes with computers has increased to almost sixty percent (United States. Census). However, this number is greatly affected by the amount of income received for each household. The Internet's original purpose was to allow researchers to exchange data more easily. As one can see, the web has come a long way since. The most prominent uses of the Internet include emailing and instant messaging, finding information in search engines, ("Internet Activities") and playing games, surfing,

and shopping (McGann). According to Rob McGann, the primary use of the Internet today is to communicate, because of the ability to convey information instantly from one person to another. Surprisingly, of these people who chat using the Internet, close to twenty percent of them talk to someone they have never met face to face and "…one out of every eight [internet users under the age of eighteen] communicate with someone they first met online" (McGann).

Even with the rapid production of twenty-first century technology, the Internet has managed to keep up, if not lead the way, with a new version of the web. Since the demand for easier more rapid communication has increased, the Internet has been able to meet these demands with the cross from web 1.0 to web 2.0. Web 2.0 can have a variety of definitions depending upon whom you ask. In simple terms, web 2.0 can best be defined as the refined and up-to-date version of web 1.0, tweaked to meet the rising demand for a better more highly social Internet. Web 2.0 includes all of today's most popular websites, primarily social networks such as Myspace, Facebook, Stickam, Youtube, SecondLife, and others.

One may ask why teenagers like using web 2.0 so much. Don Cantrell, Internet Safety expert with the South Carolina Department of Education, responds to this question with six basic reasons: they can be whoever they want, they can be friends with anyone, anywhere, anytime, they can keep in touch quickly, the Internet is an easy venue for attention, it satisfies curiosity cravings, and it's cool. The attention the Internet is capable of providing has also been referred to as an Internet user's fifteen megabytes of fame (Cantrell).

Predators

One of the five most prominent underlying dangers of the Internet is the common confusion between fantasy and reality. The lack of face-to-face or voice-to-voice contact can, and has proven to, lead to "…a loss of normal social inhibitions and constraints" (McGrath and Casey 85). Because the Internet provides an enhanced sense of safety and privacy compared to communicating face-to-face, people have been known to become more intimate more quickly, as well as contact an underage victim instead of remaining quiet (McGrath and Casey 85). Astonishing evidence shows that predatory actions are being supported by websites and groups, encouraging some offenders to act upon their fantasies with direction and support from other predators. Michael G. McGrath and Eoghan Casey recognize that, "By reducing disincentives, the Internet effectively dissolves the boundaries between fantasy and reality, enabling individuals to explore and realize their fantasies. A man who would never approach a child in the real world, may make such contact in cyberspace just to see what might happen" (McGrath and Casey 85). Another major issue with communicating on the Internet is loss of one's ability to analyze facial expression, tone of voice, and body language (McGrath and Casey 85).

One out of every seven kids has received a sexual message online (Cantrell). Almost ten percent of kids between the ages of twelve and fourteen admit to having received a request from someone on the Internet to send a nude photo of themselves (Cantrell). Michael G. McGrath and Eoghan Casey also believe that, "The anonymity of the Internet has allowed those with rare or bizarre sexual needs a place to find 'virtual' companionship, validation, and possibly an outlet for their paraphilias" (86). Thus, the Internet provides an ideal virtual world and a rich feeding ground for predators and

stalkers. The web can also provide all the support, guidance, and anonymity these activities demand.

A sexual predator, as defined by McGrath and Casey, is “a sex offender who takes advantage of a characteristic (or characteristics) of a victim to further sexual exploitation of the victim, with some element of planning involved. The characteristic can be emotional, psychological, physical, or any combination of these” (86). The mind of a predator is often times aware, organized, and extremely intelligent. The typical order of events of a predator begins with researching and finding as much personal information on a victim as possible (McGrath and Casey 87). The predator then uses the information to reel in the victim and get their trust, then proceed to gradually gain control over him or her. Providing plenty of information and data for any predator, social networking sites, including Myspace and Facebook, give these criminals an insight into their victim’s personal, social, and emotional life (Edwards 78). The youth who put details of their lives and photos of themselves on the Internet do not always think about how available the content they are posting is to the general public, and risk attracting attention from the wrong people.

The Internet has, and continues to, become a powerful tool for these criminals, allowing them to contact victims over long periods of time with out having to reveal their true identity. Therefore, the predator is able to take as much time as needed to gain trust and control over the victim. The term for developing a victim’s trust in the world of predators is called grooming (McGrath and Casey 87). Grooming reduces the chance of a victim reporting the online predator (McGrath and Casey 87). This process involves exploiting a victim’s feelings, such as loneliness, low self-esteem, and sexual curiosity,

and taking advantage of their vulnerability in order to create a bond (McGrath and Casey 87).

The Internet provides a world where sexual predators can share information and stories with other predators (McGrath and Casey 87). The Wonderland Club is an international online club for sex offenders, containing hundreds of members from around the world. A few members of this club own production facilities, where they receive instructions from other offenders to transmit live child-sex shows through the web (McGrath and Casey 88).

For years it has been common among youth to share provocative and sexy pictures of themselves with one another, but now if the sender is under eighteen their actions may result in child pornography charges (Burrell). In Ohio, during the 2008 year, a fifteen year old girl was charged, after sending her friends nude pictures of herself through her cell phone (Burrell). The charges change severely when brought up in an adult court, introducing a lifetime of registering as a sex offender along with jail time (Burrell).

Stalkers

Stalking is defined as “The repeated uninvited monitoring and/or intrusion into the life and activities of a victim that is usually, but not always, undertaken for the purpose of frightening or intimidating the victim or those around the victim” (McGrath and Casey 88-89). Cyber stalkers use the Internet to gather information on or closely monitor a victim. Obsessed harassers can be categorized into three types: the violent harasser, the love harasser and the simple harasser. A violent harasser is one who uses

aggression, anger and sometimes threats when harassing a victim. On the other hand, a love harasser is very obsessive and believes themselves to be in love with the victim. This type of harasser is often times very controlling and jealous, noticeably, or behind the victims back. A simple harasser is one who does not lean toward love or violence but is simply obsessed with harassing their victim.

One of the primary goals of an on-line stalker is to gain power over a victim, most often times through the use of fear. Keeping in mind that these victims can range from ex-girlfriends or boyfriends to teenagers and even co-workers. Not all stalkers or harassers have sexual intentions:

> One individual posed on-line as his victim, posting personal advertisements with her address and phone number, soliciting people to fulfill a rape fantasy. The victim became alarmed when men began showing up at her apartment. One of them explained that he was responding to her personal ads. When she put a note on her door to discourage visitors, the harasser posted messages on the Internet claiming that the note was part of her fantasy and should be ignored (McGrath and Casey 89).

When connected to the Internet, computers hold information on the user's activities giving an investigator of a crime insight into the criminal's interests, such as, their hobbies, fantasies, and communications (McGrath and Casey 92). Computers usually keep detailed logs of which computers attempted to communicate with them at a specific time (McGrath and Casey 91). On multi-user systems, "There is often a record of who logged in when, and even what commands were executed. Every time an e-mail server sends or receives e-mail, details regarding that message are noted in a log file"

(McGrath and Casey 91-92). With this kind of data, an investigator has the ability to not only examine the actual messages that an e-mail server contains at any given time, but also determine what messages passed through the system (McGrath and Casey 92). Even if a message has been deleted from the server to conceal a crime and is unable to be recovered, it is possible that evidence of its existence still lies in the server's log files with information on when an individual checked his or her e-mail (McGrath and Casey 92).

Identity Theft

Identity theft is defined as a "…crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain" (National Crime Prevention Council). In July 2003, a study by Gartner Research and a study by Harris Interactive showed that within the last year approximately seven to ten million people had their identities stolen. After some math, "That works out to 19,178 victims per day, 799 per hour, [and] 13.3 per minute" ("ID or Identity Theft Statistics"). The following year, in 2004, the number of identity theft incidents rose to nine-point-three million Americans ("ID or Identity Theft Statistics").

According to the Federal Trade Commission (FTC), "The total U.S. annual identity fraud cost in 2004 was $52.6 billion, an increase of 2.3% from the 2003 inflation-adjusted level of $51.4 billion" ("ID or Identity Theft Statistics"). From data collected, the cases where the method of obtaining another's identity was known less than twelve percent of the time, the information was obtained online, and offline nearly seventy percent of the time ("ID or Identity Theft Statistics"). These offline methods include

stolen or lost wallets, stolen mail from the garbage or mailbox, or by someone an individual inappropriately trusts. In fact, approximately half of all identity thefts are committed by someone the victim knows (National Crime Prevention Council).

Identity theft is becoming more common with individuals under the age of eighteen because this gives the criminal a better chance of not getting caught. In fact, there are more than fifty thousand stolen identities from minors each year (Cantrell). The signs include a minor having a credit report or the youth receiving credit card applications in the mail, and unsolicited phone calls (Cantrell).

The victims say that the emotional effect of having their identity stolen is equal to the effect of being the victim of a violent crime. For each victim the average financial loss was one-thousand-four-hundred-forty dollars (National Crime Prevention Council). The easiest way to avoid being a victim of identity theft is to be very cautious when giving out financial or personal information on the Internet. Instead, contact necessary people using a telephone or in person, ensuring that the one who initiated the call is not the thief. In addition, when one is preparing to sell, or get rid of their computer, they must be sure not to simply erase the hard drive, but to remove and completely destroy it.

Lingering Information

In his book, The Future of Reputation, Solove notes that, “Despite the fact that we talk about reputation as earned and the product of our behavior and character, it is something given to us by others in the community” (33). Once an individual places any type of information onto the Internet, it is no longer theirs and they have no control over what happens to it (Cantrell). The problem with putting too much information on the

Internet not only lies in the present but also in the future. As both a curse and a gift, the information people are so freely giving out, including pictures, blogs, and messages, is more permanent than users realize. In all reality, even if one believes they have removed this type of information, it almost never goes away completely (Cantrell). Despite how useful this can be to law enforcement agencies in efforts to track down criminals, lingering information has recently become an inconvenience to law abiding individuals primarily for job searchers and college applicants. Considering that for sometime now youth have been taking photographs of themselves and their friends practicing illegal acts. Only recently have they been able to release these pictures to such a broad and public audience. These teens and young adults frequently either do not consider or simply do not care about the possible consequences of their actions.

Within the past few years, a young girl about fifteen years of age posted pictures of herself smoking marijuana, on Myspace, while babysitting (Edwards 78). After the police were informed and looked over the photos, she was arrested (Edwards 78). Jackie Burrell notes that it is in one's best interest to not, under any circumstances "…post dicey photos or racy prose on social networking sites, no matter how private teens may think they are." A Kaplan study, in 2008, found that one in ten college admissions officers regularly check out the profiles and any other online information on their applicants (Burrell). Of these admissions officers, thirty-eight percent of them found evidence that reflected poorly on an applicant, including, talking poorly about colleges they have visited (Burrell). However, it has recently been noted that admissions officers are not the only ones checking out upcoming college freshmen. After looking over their future roommates, students at the University of Redlands confronted college administrators

about the alarming pictures and comments they found. As a result, they called up the teen's parents a few weeks before the beginning of school to confront them about the issue. In addition, the information one puts online today could some day hurt ones chances of being accepted into business or medical school, or beyond.

Lingering information can also cause a problem when searching for a job or career. Just like college admissions officers, employers are more frequently checking out applicants for jobs. Profiles can come back to haunt people who have already been into trouble with the law. There was a case in Rhode Island where a twenty year old, after consuming too much alcohol at a party, caused a car accident which severely injured another person. Burrell states that "one of the first things attorneys do with a new case is search online for information about plaintiffs, defendants and witnesses alike." After reviewing the youth's Facebook, the prosecutor found a picture of the defendant at a Halloween party dressed up as a prisoner, while the victim was still recovering in the hospital (Burrell). Because of his immature decision to post the picture on Facebook, instead of receiving a light stint at county jail, the irresponsible youth was sentenced to two years in state prison (Burrell).

Phishing

Oak defines phishing as a "…fraudulent activity of acquiring sensitive information by the use of a fake identity during electronic communication. It is implemented by means of emails and instant messages wherein a user is lured to enter his/her details, which are actually captured by a fraudulent website." According to McGann, "Spam accounts for five minutes of every hour spent online, which translates

into 10 8-hour workdays per year." Spam is another name for unwanted emails with advertisements and fraudulent claims. These "Phishers" are criminals who are out to get any personal information they can, including passwords and financial data. They do this by luring their victims into traps, using emails, advertisements, and other sources, which lead the victims to believe are from trusted company names.

Each day fifty-nine million phishing emails are sent, and one in one-hundred-forty-four emails are malicious (Cantrell). Often the email will contain the names of actual employees of the company portrayed (United States. Securities). This is done to insure that if the recipient of the fraudulent email looks to confirm an employee's existence, the person will receive an assuring answer (United States. Securities). In most cases, the fraudster, pretending to be an employee representing a legitimate company, will be informing the recipient of an issue that has come up that needs urgent attention. Somewhere in the fraudulent email will usually be a link to what appears to be a legitimate website, such as an address with the name of the company. However, to confirm the authenticity of the link, one should hover over the link with the mouse. If one does click the link, they will not be sent to the actual company's website, but an almost exact copy created by the fraudster (Edwards 7). Once at the website, like most companies who require a login on their webpage, the phisher will ask for a username and password. However, once entered, that personal information will instantly be handed over to the criminal himself (Edwards 7). When attempting to determine a phishing email, look for messages that claim: "…failure to respond will result in your no longer having access to your account … [or] that the company has detected suspicious activity in your

account or that it is implementing new privacy software or identity theft solutions" (United States. Securities).

Despite how effective this method of gaining millions of individual's personal information is, it is not the only way. Some emails do not even require the recipient to enter information. Once the victim has accessed the webpage, the site, already infected with spyware, can try to download unwanted programs to your computer, otherwise known as a drive-by download (Edwards 7). Even these methods are not enough for phishers. They are now finding ways to infect legitimate websites.

Attackers committing these crimes hardly ever launch attacks from their own computer or home, because doing so would drastically increase their chances of being located and arrested (Edwards 7). Edwards claims that instead of using their computers "…they hijack other people's computers to do their dirty work" (7). When spam and viruses first began, all they did was damage and destroy files, causing easily noticeable problems (Edwards 7). In today's hacking world, the Trojans, viruses and other harmful software have a job to accomplish; making money by hijacking. Oak defines hacking as "…the activity of programmatically gaining access to a computer application that is otherwise inaccessible." During the 1990s, the purposes behind creating them, according to Edwards, were to cure boredom, seek fame, explore the possibilities of the Internet, cause trouble, and simply create peer pressure (8).

There are three types of malware: trojans, viruses, and worms. Having been around for a long time, viruses have become very advanced. They can target and infect USB flash drives when inserted into an infected computer, and spread to every computer it is inserted into; a terrible and sinister tool for force of corruption (Edwards 28).

Internet users should always be aware that whenever one downloads anything from the Internet, even though they may receive what they want, the downloaded material may also have an unwanted friend joining in on the ride. Trojans, or trojan horses, do not always become active when first received, making there presence less obvious. They hide in the memory of a computer and wait there patiently for the owner to do something worth noting; then send the gathered information back to the criminal. At that point, the criminal has a choice to either use the information to steal money for his or her own purposes or sell the information to various sources in online gangs who work together (Edwards 9). On the Black Market, an individual's social security number goes for about ten dollars. It is scary to think that in terms of money, manpower, and effectiveness, it is more efficient "…to attack central services over the Internet than to send in suicide bombers" (Edwards 12). In fact, Al Qaeda uses chain mail to transmit information using codes through pictures. So next time you get an email telling you to forward it to ten people or your boyfriend is going to break up with you tonight at eleven forty three, just delete it.

Unlike viruses, trojans do not spread automatically; they rely on their attractiveness to lure in their victims. Worms, however, do spread automatically, using the Internet and internal networks to jump from computer to computer (Edwards 28). The best way to avoid worms is to use a firewall.

To avoid unwanted malware, it is a best practice to keep anti-virus software and firewalls up to date, disregard emails from strangers, and do not leave one's computer connected to the Internet (Edwards 30-31). When checking the legitimacy of a web address, the user can almost always count on a safe website when "https" are the first five

letters (Cantrell). The “S” marks websites that have been officially checked out and approved as secure (Cantrell). The user can also verify emails and websites at snopes.com, a reliable and popular resource for determining the accuracy and truthfulness of email or web content (Cantrell).

Cyberbullying

In the little town of Essex Junction, Vermont, thirteen year old Ryan Halligan began talking to a girl in his school who he believed was starting to show interest in him (Makenna). Little did he know, she was printing and sharing the messages they had been exchanging over the Internet with her friends, who had been taunting and spreading rumors about him, saying he was gay. Ryan killed himself, unable to deal with the trauma (Makenna). Since Ryan’s tragic death in 2003, the number of youth accessing the Internet is growing at a steady rate, along with online bullying.

When anyone under the age of eighteen is threatened, humiliated or harassed by another minor, this is considered cyberbullying (Surdin). Cyberbullying can range from sending threatening messages, sharing private messages, spreading rumors, and posting embarrassing videos or photos online (Cantrell). It has gotten to the point where teenage girls are feeling forced to strip by their boyfriends and the videos are ending up online after falling into in the wrong hands (Cantrell). Commissioned by the National Crime Prevention Council, a study in 2006 revealed that four in ten teenagers reported experiencing some form of cyberbullying (Surdin). The data also showed that cyberbullying is most common among girls between the ages of fifteen and sixteen (Surdin).

Because of anonymity, the Internet magnifies the effect of bullying on a victim. An individual's ability to remain nameless and faceless takes down boundaries and allows them to act in ways they otherwise would not, and even reach higher levels of cruelty (Makenna). Results also show that the intensity of cyberbullying is capable of leading to failing grades, skipping classes, and thinking about suicide (Surdin). In Makenna's article, Kowalski claims, "The psychological ramifications of not knowing who is attacking you can be maddening." The results of one of her surveys showed that half of the victims of cyberbullying had no clue who the bully was (Makenna).

Within the past year the push to drastically reduce cyberbullying has become a priority in the United States. Recently people are asking for laws that target school districts to require educators to come up with rules against cyberbullying and resources to train the staff (Surdin). As of January 2009, thirteen states, including South Carolina, have passed laws allowing districts to punish students who commit such acts, while many other states are seriously considering doing so (Surdin). The primary reason some schools are reluctant or unsure how to approach this issue is because the line between harassing and practicing free speech has yet to be defined (Surdin). Aden Fine, a senior staff lawyer with the national legal department of the American Civil Liberties Union, defends the right of free speech and believes that a problem with these laws is that they allow the schools to attempt to control what students say outside of school (Surdin).

Though primarily an issue for teens, cyberbullying can affect adults, including celebrities, teachers and coaches. In 2006, the United States Congress made it illegal for anyone over the age of eighteen to abuse, annoy, harass, or threaten another person using the Internet. Once placed on the Internet, gossip can cause "…a permanent reputational

stain" (Solove 33). One should always think twice about whether it is truly worth it to post gossip and jokes online, who all can see and read them, and what effect the comment might have.

Conclusion

As the Internet becomes more accessible to individuals across the world, it is more important for all generations of Internet users to understand the playing field before becoming a part of the online world. Through the increasing number of Internet users and the various uses of the Internet, to know even the most basic, but necessary, background knowledge can steer you away from the harmful effects of the Internet. In order to have the most safe and successful internet experience that one can, it is important that the user be aware and know how to steer away from and, if ever confronted, deal with predators, stalkers, identity theft, lingering information, phishing, and cyberbullying.

Work Cited

Bellis, Mary. “The History of Computers.” About.com. 22 Jan. 2009 <http://inventors.about.com/library/blcoindex.htm>

Burrell, Jackie. “Facebook, MySpace and Internet Perils: 5 Online Dangers That Have Nothing to Do With Internet Predators.” About.com 2009. 13 Jan. 2009 <http://youngadults.about.com/od/legalissues/a/facebookcaveat.htm>

Cantrell, Don. “Socializing on the Internet.” Office of Safe and Drug Free Schools, Hand Middle School. 22 January 2009.

Edwards, Simon, ed. The Complete Internet Security Handbook 2009. London: Dennis, 2008.

Holmes, Gary. “TV, Internet and Mobile Usage in U.S. Keeps Increasing.” Nielsen. 23 Feb. 2009. 14 March 2009 <en-us.nielsen.com/main/news/news_releases/2009/February/tv_internet_and_mobile>

“ID or Identity Theft Statistics — Are You at Risk?” PrivacyMatters.com 4 Dec. 2006. 8 Jan. 2009 <http://identity.privacymatters.com/identity-articles/identity-theft-statistics.aspx>

“Internet Activities.” PewInternet. 15 Feb. 2008. 22 January 2009 <http://www.pewInternet.org/trends/Internet_Activities_2.15.08.htm>

Makenna, Phil. “The Rise of Cyberbullying.” Newscientist.com 19 July 2007. 11 Jan. 2009 <http://www.newscientist.com/article/mg19526136.300-the-rise-of-cyberbullying.html>

McGann, Rob. “Internet Edges Out Family Time More Than TV Time.” ClickZ. 14 Nov. 2008 <http://www.clickz.com/showPage.html?page=3455061>

McGrath, Michael G., and Eoghan Casey. “Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace.” J Am Acad Psychiatry Law 30:81–94 (2002). 7 Jan. 2009 <http://www.jaapl.org/cgi/reprint/30/1/81>

National Crime Prevention Council. Preventing Identity Theft: A Guide for Consumers. Washington DC: Bureau of Justice Assistance, 2005.

Oak, Manali. “Basic Internet Terms and Terminology.” Buzzle.com 4 Oct. 2008. 8 Jan. 2009 < http://www.buzzle.com/articles/basic-Internet-terms-and-terminology.html>

Solove, Daniel. The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. London: Yale University, 2007.

Surdin, Ashley. “In Several States, A Push to Stem Cyber-Bullying.” The Washington Post 1 Jan. 2009. 11 Jan 2009 <http://www.washingtonpost.com/wp-dyn/content/article/2008/12/31/AR2008123103067.html>

United States. Census Bureau. Typical Daily Internet Activities of Adult Internet Users: 2006. 19 Dec. 2008. 11 Jan. 2009 <http://www.census.gov/compendia/statab/2008/tables/08s1130.pdf>

United States. Securities and Exchange Commission. “‘Phishing’ Fraud: How to Avoid Getting Fried by Phony Phishermen.” Sec.gov 23 Aug. 2007. 13 Jan. 2009 <http://www.sec.gov/investor/pubs/phishing.htm>