ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
September 2013,
Vol. 6, No. (3):
Pgs. 295-302

Dangers of Internet to Society and Practical Avoidance

**MOHAMMAD. AL- RABABAH, ABDULSAMAD AL-MARGHIRANI
and MOHAMMED MOSA AL-SHOMRANI**

Northern Border University, KSA
King Abdul-Aziz University, Jeddah 21589, KSA

(Received: August 20, 2013; Accepted: September 15, 2013)

ABSTRACT

The internet information network of the latest technology at the moment, which is linked to information and communication technologies and computers that have evolved significantly since the end of the last century, and continues to evolve quickly and persistence. Some Statistics indicate that the number of Internet users in the world, about 0.7%, while in the United States and Canada, up to 40% . The online network is composed of huge numbers of networks, linking computers distributed in different parts of the globe, dubbed the “network of networks”, because most of the computers connected to the Internet, are also part of smaller networks, found within companies, universities and government departments, and connects online between these networks to make up the global network is huge, connects hundreds of millions of people, to communicate with each other, and access to information, and the exchange of data and programs, and serves the Internet more than 200 million users and is growing very fast up to 100 percent per year, has started the idea of the Internet was originally military government idea and spread to the education sector and research and then trade up to become accessible to individuals where the sail in the Internet completely free but the price you pay is to provide a service to you.

Key words: Online dangers; Internet risks; Social risks; Dangers to society.

INTRODUCTION

This paper discusses the dangers to society by using the Internet as the communication channel. The social risks involved in using internet’s popular services like online chat, blogs, Internet gaming and Internet gambling are vary and highly correlated. This study analyzes each of these social risks and illustrates various solutions to overcome these dangers.

Although there are risks associated with the use of the Internet as an effective communication technology, most of them can be moderated with an organized and systematic approach, including both technology and social consciousness (Sherri and Jonathan, 2012; Bass, 2009).

Vulnerability of Social Networking Sites

Social networking sites are Internet-based services that allow people to communicate and share information with a group .

Risks

Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high security settings, friends or websites may inadvertently leak your information

Personal information you share could be used to conduct attacks against you or your associates. The more information shared, the more likely someone could impersonate you and trick one of your friends into sharing personal information, downloading malware, or providing access to restricted sites Predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site

Tactics

Baiting

Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer Do not use any electronic storage device unless you know its origin is legitimate and safe. Scan all electronic media for viruses before use

Click-jacking

Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed “Like” and “Share” buttons on social networking sites. Disable scripting and iframes in whatever Internet browser you use. Research other ways to set your browser options to maximize security.

Cross-Site Scripting (XSS)

Malicious code is injected into a benign or trusted website. A Stored XSS Attack is when malicious code is permanently stored on a server; a computer is compromised when requesting the stored data. A Reflected XSS Attack is when a person is tricked into clicking on a malicious link; the injected code travels to the server then reflects the attack back to the victim’s browser. The computer deems the code is from a “trusted” source .

Doxing

Publicly releasing a person’s identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles Be careful what information you share about yourself, family, and friends (online, in print, and in person).

Elicitation

The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated. Be aware of elicitation tactics and the way social engineers try to obtain personal information

Pharming

Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential data. (E.g.: mimicking bank websites.) Watch out for website URLs that use variations in spelling or domain names, or use “.com” instead of “.gov”, for example. Type a website’s address rather than clicking on a link. For examble**:**

Most computer infections come from websites. Just visiting a website can expose your computer to malware even if you do not download a file or program. Often legitimate sites may be unknowingly infected. Websites with information on popular celebrities or current sensational news items are frequently hijacked by criminals, or criminals may create such websites to lure victims to them.

Phishing

Usually an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim . Do not open email or email attachments or click on links sent from people you do not know. If you receive a suspicious email from someone you know, ask them about it before opening it .

Example

In March 2011, hackers sent two spear phishing emails to a small group of employees at security firm, RSA. They only needed one employee to open an infected file and launch the malware. The malware downloaded information from RSA that then helped the hackers learn how to defeat RSA's security token. In May and June 2011, a number of defense contractors' networks were breached via the compromised RSA token.

Phreaking

Gaining unauthorized access to telecommunication systems Do not provide secure phone numbers that provide direct access to a Private Branch Exchange or through the Public Branch Exchange to the public phone network

Scams

Fake deals that trick people into providing money, information, or service in exchange for the deal If it sounds too good to be true, it is most likely a scam. Cybercriminals use popular events and news stories as bait for people to open infected email, visit infected websites, or donate money to bogus charities .

Example

Before the 2010 World Cup, cybercriminals offered tickets for sale or sent phishing emails claiming you won tickets to see the event. After the death of Osama Bin Laden, a video claiming to show Bin Laden's capture was posted on Facebook. The video was a fake. When users clicked on the link to the video, they were told to copy a JavaScript code into their browser bar which automatically sent the hoax to their friends, and gave the hackers full access to their account.

Spoofing

Deceiving computers or computer users by hiding or faking one's identity. Email spoofing utilizes a sham email address or simulates a genuine email address. IP spoofing hides or masks a computer's IP address . Know your co-workers and clients and beware of those who impersonate a staff member or service provider to gain company or personal information

Chat online

Today have found a common hobby-chatting online. This has come about with the growing numbers of readily downloadable and user-friendly programs online such as the Internet Relay Chat (IRC), I Seek You (ICQ) and Microsoft messenger (MSN messenger). Users are free to discuss any topic with anyone in the chat rooms. Most teenagers find the relative anonymity and convenience of chatting online fun and interesting but many do not realize or disregard the dangers online chatting pose. In this article, I shall examine the dangers of chatting online and how readers can avoid them. While Chatting Online, teenagers tend to confide their lives' problems, their thoughts and feelings to chatting partners moments after starting their conversation. In doing so, they often perceive a close relationship with their chatting partners. That is, good friends whom they can always confide in or even as a boyfriend/girlfriend. There is also a high propensity for teenagers to give out personal information like their mobile phone number and where they live, to chatting partners. The problem with online chat is people usually only "see" a sugar-coated version of their chatting partner

The risks of online chat include:

Internet stalking

There is global communication through the Internet. Here the domain is more wide and public in comparison to e-mail stalking. Here stalkers can use a wide range of activities to harass their victims. For example, harasser may post notes in a chat room that threatens to intimidate and kill the victim, or post altered explicit pictures of victim on the net together with personal details. While indirect cyber stalking includes the use of the Internet to display messages of hate and threats or used to spread false rumours about a victim. Statistics show chat rooms, instant messages and message boards, to be the most common way that indirect cyber stalking begins (Debra and Michael, 2008).

Exploitation of Children and Teens

In Instant Messaging and chat room conversations, Pedophiles and offenders often pose as young child and get a child to speak to them. The child may unintentionally provide personal information such as location, phone numbers, or email addresses to these offenders. Preferential offenders use the technology to groom any number of potential victims over a period of time (Thomas *et al*., 2009; Monique *et al*., 2005). Offenders have been known to groom as many as fifty or sixty potential victims at a time. Self reports by offenders indicated that they might carry on Instant Message and chat conversations with more than twenty potential victims at any given-time.

Online Libel

Libel means the defamation in a permanent form (Thomas *et al*., 2009). This includes comments made online, including comments made in a chat room or in emails or on websites.

Commercial software can monitor online behaviors, including e-mail, chat room conversations, instant messages, passwords, and Web site visits. Some software can record keystrokes. Most monitoring software allows the installer to guard access to it with a password.

Fig. 1: Show online chat

Blogs

A blog is an online journal which allows people to express their thoughts and ideas. Blogger must be careful not to reveal too much personal information and to protect their reputation (Keating et al., 2009; OECD, 2009). This is important because many educational institutions and companies now conduct online searches of prospective students and employees. The consequences of indecent blogging could negatively affect a person’s academic or career future.

Blogging risks

Even if you blog anonymously,

Your details can be discovered. This is possible if your blog is not covered under data protection or privacy laws as in US or UK.

Libel laws are applicable to blogs

Inappropriate blogging about a person or company may incur serious penalties.

Be careful while blogging about your job.

You may lose your job because of an inappropriate post.

Many blogs have ‘comment’ feature

This may be exploited by spammers and other malicious individuals to promote fake or fraudulent websites.

Unwittingly posting personal information or photographs of themselves by the youngsters.

Risks of cyber stalking

Risks off online bullying

Unauthorized disclosure of business information and potential confidentiality breach in corporate blogging.

Malicious attack associated with identity theft.

Avoidance of blogging risks

Follow these steps to avoid the risks associated with blogging:

Provide minimum information while creating online profile.

Post your blog anonymously

Avoid personal information or identifying details and photographs.

Refrain from inappropriate comments that may provoke others.

The games of internet

Become online games are the most

common and popular entertainment on the Internet so as to offer now in the areas of communication and Internet high speeds and today in games but very cybercriminals see them very profitable and a great opportunity to earn a lot of huge amounts of money illegal and must player in online very careful because they introducing technological and social risks associated with each other.

The risks of the gamers include

The gamers involve the following technological risks to their computer system and the systems which they connect.

Viruses, trojans, worms and malicious software

Malicious programs or viruses may enter your system as hidden files while you download or install the gaming software. Sometimes online criminals may use the social network associated with the gaming programs which provide features like email, instant chat or voice communication to lure you to open an email attachment or visit a fake website which may contain malicious software and install on your system. Thus the intruder can remotely control your system and use it for various illicit activities (Sherri and Jonathan, 2012).

Buggy gaming codes

Bugs in the gaming code may arise various security threats as well as other unknown vulnerabilities to the gamers' computer system and the other systems to which they communicate.

Insecure online game server

All Massive Multiplayer Online games (MMOs) have a certain level of risk to security. If the game server becomes insecure, the. By taking advantage of these vulnerabilities, malicious intruder might be able to attain total control of your system remotely and use it to attack other gaming computers or install malicious programs or gain access to your personal and financial information on your computer system.

Now we will discuss Social risks

Malicious intruders may sometimes exploit the security vulnerabilities of the social interaction features of the online gaming environment to get control over the victims system. These intruders may do these:

- Steal your financial information like account numbers, credit card numbers etc.
- Gain access to your personal information.
- Identity theft.
- Establishing contact with the children using fake identities, sometimes causing personal harm to the children.
- Blackmailing other gamers.
- Stealing other gamers points or game items, also called "virtual mugging".
- Gaming addiction causing serious health and psychological problems.

Technical approaches for avoidance

Avoidance of technical risks is to implement and follow key practices of good computer and network security measures.:

Use "user-mode" instead of "administrator-mode" while gaming, which is safer. Otherwise, if your system is compromised then the intruder may system in the administrator mode.

Use and manage firewall properly. The exception list in the firewall should be managed carefully. Better add specific IP address of the fellow gamers in the trusted list which may reduce the risk of malicious intruding.

- Aware of the risks associated with Active X and JavaScript before enabling it.
- Use 'internet security suites' which is updated properly.
- Back-up your data.
- Do not open attachment from email and IM which is not safe.
- Verify the authenticity of files and software downloaded.
- Use strong passwords and change it frequently.
- Use the latest updates and patches for the web browsers and other application softwares and configure it securely.

Internet Gambling

In little more than a decade, online gambling has exploded from a minor sideshow on the Internet into a substantial global industry. During that time, the United States has struggled to develop a comprehensive policy on Internet gambling. Indeed, federal and state governments have applied fragmented and sometimes inconsistent policies to this new technology for delivering a very old form of entertainment. For example, the government's attitude toward online gambling has been largely hostile including indictments of major offshore gambling operators but it has allowed the horseracing industry and state lotteries to conduct online betting. Because of the enduring popularity of poker in America, this paper will focus on current proposals to legalize only online poker, with particular emphasis on what we have learned since the Unlawful Internet Gambling Enforcement Act (UIGEA) became law five years ago. The broad availability of Internet gambling sites around the world has provided a real world study of the different ways for public policy to respond to online gambling

That experience teaches three basic lessons

´ Millions of Americans have continued to bet billions of dollars a year at offshore websites. Americans like to gamble online and have demonstrated that they will do so even if their government tells them it is illegal. Although criminal prosecutions and legislation can cause the volume of online gambling to fluctuate in the short run, the track record shows that the demand for online gambling remains, and offshore operators will figure out ways to meet that demand.

´ The current policy on Internet gambling ensures that foreign nations and foreign businesses reap the benefit of the jobs, economic opportunities and tax revenues that are generated by Americans' online gambling. Legalizing online poker will create, directly and indirectly, an estimated 10,000 high-tech jobs in this country, the sort of jobs that our citizens urgently need.

And it will generate an estimated $2 billion of tax revenue every year for state and federal governments, helping preserve critical public services in a time of increasing budgetary constraints.

´ Well-designed regulation can control the social risks that some fear from the legalization of online gambling. Based on years of experience with regulated online gambling in the horseracing and lottery sectors in this country, and with legalization in some Canadian provinces and in Europe, we know that a strict regulatory system can ensure that online games (i) are fair to players, (ii) exclude minors, (iii) provide tools that allow customers to limit their gambling, or self-exclude entirely from online gambling; (iv) exclude bets from jurisdictions where online gambling is illegal, and (v) prevent the use of online betting sites for money laundering or other illegal purposes. Indeed, if online gambling is not legalized and regulated, Americans will continue to gamble online at websites that are based in jurisdictions that provide the least protection for their customers and create much higher risks from online gambling.

Technical approaches for avoidance

To avoid 'gambling by minors', researchers have outlined several categories of technologies for verifying the age of adults, including comparison of the registrant's credentials against public databases such as credit reports and criminal histories, or even biometrics. An age-verification service is used to check the information provided against a database containing credit data, driver's license data, and registered voter information.

´ Establish regulatory and monitoring bodies to control the different

´ Personal and financial information of the gamblers must be treated with extreme caution. Effective data protection begins with the establishment of internal controls and policies by the gambling website.

´ The key technologies for gambling website include (4.2.4.1) network firewalls that isolate databases, administrative systems,

´ date security patches,

´ a continuing process of monitoring and logging attempts to break into the system over the Internet,

´ secure database and transactional software, and

´ the use of secure, encrypted protocols for communications between users and the gambling website.

This paper illustrates some important topics concerning the potential social risks involved in internet's popular services like online chat, blogs, Internet gaming, Internet gambling. One of the methods to curb the dangers of internet to the society is to create a social awareness among the people to refrain from the negative aspects of the internet (Wen et al., 2007). Here we discuss various social approaches to overcome these dangers.

a) Awareness in school level: In many cases, children and teenagers are the victims of cyber crime. School authorities/educators, Social and religious organizations and law enforcements can do reasonable things in reducing these risks by including specialized courses in the curriculum like 'Internet and Society' that may give an in depth idea about the positive and negative aspects of Internet, lectures by social and religious bodies and the support and advise to the victim from the law enforcement department (EURYCIDE, 2009).

b) Creating awareness in the society: Social reformers, religious bodies and law enforcement forces can conduct lectures, distribute booklets and place informative programs in popular web portals and visual media like TV.

c) Penalties of Internet crime: The law enforcement bodies should provide lectures to make the society aware about the punishments involved in various cyber crimes.

d) Publicize the detail of the criminals: Through public websites and medias publicize the details of criminals and the penalties they incur so that the society must know what is the outcome of such online crimes.

e) Parents and responsible adults: at first, they can make themselves aware of the potential online dangers and the ways to report online crime, talk openly with their children about Internet dangers (Davies and Good, 2009).

Fig 2 : Show internet Gambling

CONCLUSION

The internet offers numerous opportunities for knowledge gathering, entertainment, and social interaction. Of course, there are many positive aspects achieved from the time we spent online. The risks and threats posed by the Internet leaves us no option but to strengthen the cyber security measures that can be approached technically and through promoting social awareness.

REFERENCES

1. Livingstone, S. & Helsper, E., Balancing opportunities and risks in teenagers' use of the internet. *New Media & Society*, **12**(2): 309-329 (2010).
2. Dietz P.E., Dangerous information: product tampering and poisoning advicein revenge and murder manuals. *Journal of Forensic Science* **33**(5): 1206-17 (1988).
3. EPoSS. The Internet Of Things — EPoSS. [Internet] Available at: http://www.smartsystems-\integration.org/public/internet-of-things. [Accessed 18 August 2011] (2011).
4. Bargh JA., Beyond simple truths: the human-Internet interaction. *J. Soc. Issues* **58**(1) (2002).
5. Bargh JA, McKenna KYA, Fitzsimons GM. Can you see the real me? Activation and expression of the 'true self' on the Internet. *J. Soc. Issues* 58(1) (2002).
6. Glaser J, Dixit J, Green DP., Studying hate crime with the Internet: What makes racists advocate racial violence? *J. Soc. Issues* 58(1) (2002).
7. Hampton K, Wellman B., Long distance community in the network society. *Am. Behav. Sci (*2001*).*
8. Howard PEN, Rainie L, Jones S., Days and nights on the Internet. *Am. Behav. Sci (*2001*).*
9. Jones S., *The Internet Goes to College.* Washington, DC: Pew Internet/Am. Life Proj. http://www. pewinternet.org (2002).

10. Kavanaugh AL, Patterson CJ., The impact of community computer networks on social capital and community involvement. *Am. Behav. Sci.* **45**: 496-509 (2001).
11. Nie NH., Sociability, interpersonal relations, and the Internet: reconciling conflicting findings. *Am. Behav. Sci* (2001).
12. Livingstone, S. & Helsper, E., Balancing opportunities and risks in teenagers' use of the internet. *New Media & Society*, **12**(2): 309-329 (2010).