Security on the internet research paper example

Law, Security

References: 19

Security on the Internet

The internet is an integral part of modern communication. Yet it is also the source of many security issues of private information because of its widespread nature and availability. These security issues are associated partly to the inherent characteristics of the internet and to human error (Holden, 2003). The advancement of technology has allowed services and items to be delivered through the internet by collecting information. However, such information comes with a price. In exchange of convenience, consumers become targets to cybercrimes because of the information they provide (i. e. bank account information, address, and personal identity) (Sicari, 2013). Indeed, protecting privacy on the web becomes more intricate due to the considerable amount of sensitive information provided in many locations during internet browsing. While a third party collects and compiles

data to build personal profiles of internet users to provide free and personalized services, perpetrators are lurking to gather these information without the user’s knowledge (Malandrino and Scarano, 2013). This paper presents some of the major internet security concerns and their potential solutions.

Growing Popularity on the Internet

It is clear that the ease and relative meanness of publishing information on the Internet is something that has been leading businesses and industrialists similarly to jump into Cyberspace. However, with an investment of just US$30 a month, most individuals are able to set up their own Web operations by utilizing a personal computer and a good modem (Treese, 2004). The enormous potential of customers and clients has businesses climbing to get on to the Network. Millions of individuals all over the world can look at these pages on the universal Internet. Research shows that it has turned out to be affordable and easy to get admission to the Internet and most likely customers like to look at a business that is displaying them on " the Net". Customers are able to look for the products of an organization ask questions straight to them without having to go to the waste time by going to the store.

Although the commercial market of the Internet might be small today, it is likely to grow tremendously in the future. Commerce will begin in earnest on the Web when the computer becomes as easy to use as a telephone or other household appliances. The Net itself has to become more attractive for customers, since unresolved privacy implications might hinder customers from purchasing items on the Net. The security of transactions is one aspect

and will be discussed later in this article. Another important factor is the tracking of customers. Already, companies can collect data on a person's entertainment-viewing habits, their telephone-calling patterns and their shopping behaviors. In addition, they can record the time and pages which a customer saw during his/her stay on the Web.

Old-fashioned habits of communicating and advertising with customers are no longer suitable and cannot be utilized easily on the Net. Now, companies will need to be able to come up with some new innovative methods of communicating with employees and customers all over the world.

Of course, some disadvantages for a business doing business on the Net involve the " surfing" of workers on the Net in business time (Treese, 2004). The more captivating the World Wide Web gets, the more probable workers are to do this. Personnel have to be able to self-control themselves in order to evade sitting in front of their computer looking through the Net and not really doing anything that is productive for the business. However, it has been considered that the average worker spends 10 hours per week online going through websites and answering their e-mail in business time. What's more, health-connected topics might turn out to be significant, as individuals working with computers are probable to acquiring eye-strain headaches and some form of " computer compulsion (Speed & Ellis, 2003).

Further investigation has been showing that the Internet proves very beneficial for getting rid of costs while becoming involved with customers. In order to give information on the Net, and permit customers to discover answers to their questions themselves wonderfully aids to bringing down telephone charges founded on 800 and 888 numbers. In addition, companies

will be able to also save money by contributing their software or trial types on the Internet, as individuals are able to modestly download any type of document. The business will not have to pay any type of postage any further.

Threats on the Internet

As people link a computer to the Internet, they compromise the integrity of its boundaries, resulting to the computer losing its private status. Thus, one must consider the risks of exposing private data before deciding to gain any potential benefits out of connecting to the internet. The nature of data in a healthcare environment for instance is often highly sensitive. There is also the danger of home computers exposing data, such as banking details, when connected to the internet (Kelly and McKenzie, 2002). Hughes (2008) noted various categories of potential risk when using the internet. These potential risks include: hacking, phishing, Trojan horses, spyware, adware, or malware, tracking cookies, viruses, worms, and fake programs that present themselves to combat the aforementioned risks.

Computer hacking is defined as an illegal manner to crack computers or passing through security measures. The internet serves as a ground from which many hackers launch their attacks on personal computers. The IP address of Wireless Personal Area Network and Local Area Network allows such connection of constrained devices (i. e. sensor nodes with global Internet standardized IP protocol). Routers connect these networks with the internet and because of the nature of these devices they directly connect to untrusted internet sites which makes it possible for attackers to access resource constrained devices from anywhere on the internet (Raza, Wallgren

and Voight, 2013). When the system is vulnerable hackers are able to direct attacks to a single computer. These hackers are able to identify the IP of the target computer and then gain access through a free port on the CPU. In so doing, these hackers can access private information such as credit card numbers for financial gains.

Phishing refers to the attempt of a third party to access login and password information for a specific website. Perpetrators set up false website which appears very convincing such that the users are attracted to enter their personal information. Phishing also targets “ bank websites, pay-online web sites, and any website which require credit-card numbers.” Trojan Horses are destructive programs which download themselves onto the computer as a benign application. These programs can cause various damages to the computer to include: (1) remote access to computers eventually having complete control of the system; (2) “ data sending”—where others use personal computers to obtain personal data such as credit card and social security numbers; (3) destruction of computer hard drive and data within it; (4) computer turning into a " proxy server" which set-up credit-card fraud; (4) remote connection of other to computer which allows downloads of the content of your hard drive (through FTP Trojan); (5) inactivation of security software such as firewall or security or anti-virus in the computer thereby allowing other Trojan programs or hackers to access personal information; and (6) denial-of-service attack where the virus attack an entire network system such that disabling the system will deny users to access their account (Hughes, 2008). Incidence of the latter virus damage has been reported by Brenner (2013). Since September 2012, security attacks on US

banks have disrupted services and cost US banks to defend tens of millions of dollars. Forensic experts ascribed the attacks to Iran. Denial-of-service-attacks have been occurring ferociously in the country which might take the world financial systems down. Security officers are wary of the fact that attackers are being sponsored by a country with first-rate capacity.

The adware, also known as advertising-supported software are those pop-up ads or certain types of web advertisements that appear in web browsers. This software automatically plays, displays, or downloads advertising material after installation or while certain applications were open on the computer. Pop-up ads appearing on the computer proliferates which is related to the same subject matter that is being researching. Spyware covertly installs software on a computer at the same time that another piece of software is installed when visiting a webpage. From the root word “ spy,” the aim of this software is to monitor user’s behavior on the computer, collect personal information, and interfere with the control of machine. Identity theft is one of the many threats of the spyware. Spyware can " repurpose" a computer for other services without the knowledge of the user. Malware has a similar objective to spyware, but has the goal of using one’s computer to be hostile, intrusive, or annoying on another computer. Malicious software damages one’s computer using the machine as a base (Hughes, 2008).

Viruses are the most popularly known form of intrusive attacks on computers. These viruses infect the host system (or server) of the computer. The damage continues as the host system contacts with others. Viruses travel through any type of file-transfer and travel easily through computer

networks by attaching itself to the file or the program. As a consequence, the performance of the system decreases. Worms are a variety of viruses that are self-replicating. They do not to a computer file but have their own life which destroys the entire computer networks (Hughes, 2008).

Cookies convey information between a computer and a web site. They can be benign and sometimes helpful in saving preferences for a certain website but some tracking cookies can collect personal information. Tracking cookies refers to small, discrete files that download automatically when one hits a certain website while surfing. These small files gather information about: (1) the number of times a site is visited when users make purchases; (2) other similar pages one might read; (3) ads that were clicked on; and (4) information used to complete online forms (Hughes, 2008).

Information security is founded on the following three foundations:

- Data reliability. A corporation must be sure that its facts have not been altered.
- Confidentiality of records. Corporations have to be able to not talk about the information that they are aware of such as their credit card numbers and customer database.
- Genuineness. Corporations need to make sure that messages they obtain from the Net are from the individuals that they are claiming to be.

If any of these factors are able to be worked around by hackers the organization is no longer looked at as being secure. Another threat is the growing amount of data dealers who utilize online communications to match sellers and buyers. Offenders continuously seem to be one step ahead of the game even ahead of the police.

An online Internet business likewise faces other threats that are challenging. Since workers can discover all kinds of data on the Internet, they could tend to download some material that is adult oriented adult material, which they could possibly display around within the business. Such workers are able to make a hostile working area. Further investigation shows that other workers could feel sexually harassed inside the business and could press charges against the corporation. The organization will have to make sure that workers are not able to download such photos or other violent material from the Internet (Treese, 2004). Strict guidelines will have to be developed in order to protect its own interests and the unrestrained surfing habits of its workers.

Combatting Security Threats

Research shows that wise internet surfing is more than likely the best solution when it comes to fighting to all of the security threats on the internet. Some experts believe that by this it means that a person will need to be careful when deciding to go to these internet sites. However, new evidence shows that when combined with technical insights a person is able to avoid various system issues. Research shows the simplest method way to stop hackers from coming into the system is by constantly making sure that the operating system software is updated with security patches. Also, data transmitted to and from the server will need to be encrypted with some kind of a strong signal. In return, this would make it much harder for the intruder to save the information gotten by means that are illegal.

Research also points out that checking the URL (address) of the web page where personal information was inputted to guard against phishing is also

important. This is vital to note because if the URL is not displaying the company site being access, this is saying that the user is in danger of being subject to a phishing operation. While there are web browsers phishing filters obtainable it is extremely vital to be concentrating to website speaks to when utilizing the Internet.

Research shows that servers on the internet are frequently being targeted on denial of certain kind’s service attacks. Research goes on to shows that these people that own these websites need to learn how to regularly scan the traffic to their websites and have methods of differentiating among the fake and real information. In the end, this will make sure their clients are getting enough access to their website for the next 24 hour a day.

It is obvious that computers that are being installed in the internet could be infected with Trojans. Many are unaware that Trojans are programs that are used to disguise as genuine programs in order to get access to a user’s computer. Most of the time, hackers are using these Trojans to look for monitor emails, look for instant messages or even observe database communications (Speed & Ellis, 2003). Trojans are made to negotiate a computer without being noticed by the person who owns it. Those who are users of the internet will need to be able to install some kind of strong antiviruses in their computer. When this is done it will help to detect and quarantine items discovered to contain Trojans.

People who use the internet most of the time go about their business in a state of anonymity. Many are unaware that the websites do not need for users to recognize themselves. This is saying that there is a possibility for criminals to get a hold of the internet and then start their dirty work. One of

the most typical is called the cyberbullying. Research shows that this takes place when individuals start mistreating other people especially in locations such as message boards or group chats. According to Speed & Ellis (2003) there are also potentials of pedophiles all over these websites to lure their victims. In order to fight this security measure, designers of websites will need to create it essential for people to give personal identifying date before being permitted to make any comments on their content. However, they also make the point that parents will need in order to utilize family safety features obtainable on most operating systems.

Numerous websites require ask for users to login before using their services. When that is done, people have to come up with some unique password that will give them access to their personal account (Kelly, 2002). Research shows that attackers at times will target the passwords so they can break into the user account. The brute force method is one of the approaches frequently used by attackers. However, his shows running dictionary type of words and their arrangements as the keyword in the expectation that one of them will be the right PIN. This is likely in the contemporary internet age as there are great computers that can run millions of words in a small time frame. In order for person to protect oneself from such attacks, the person using the computer will need to make a powerful password that contains the numbers, letters, and symbols (Nosek, 2012). Experts explain that of they take this route, it will make it impossible for the invaders to get a hold of the right combination.

Cyber security Threats

Cyber security is a governmental-level strategy objective. President George

W. Bush in January 2008 delivered a still-classified national security and homeland security instruction to take-off the country's Comprehensive National Cyber security Initiative (CNCI). (Speed & Ellis, 2003) After that year, the administration delivered the Cyberspace Policy Review briefing a 70-day review of cyber security rule. The Review is interesting because it set out initial near-term and mid-term action matters for safeguarding cyberspace. Research shows that central to the tactics was fastening leadership for cyber security inside the White House, predominantly by assigning a manager for cyber matters who would answer to both the National Security Council and the National Economic Council. It is understood that the military secures its own networks under the leadership of the newly-initiated United States Cyber Command, whose chief is dual-hatted as the head of the National Security Agency. Also the Department of Homeland Security is a group that does have the lead when it comes to securing federal government networks. (Holden, 2003) Ultimately, companies that are private secure their own systems. However uncertainties in one system can have an effect on another; for instance, government and military services frequently share the same public-Internet substructure as private corporations, and trust on private web services that could be compromised or attacked. More, cyber-attacks directed through uncertain private networks are able to attack armed forces networks, and vice versa. Therefore, these diverse powers that be will need to be able to work together in order to make sure each other's security is safe.

Cyber security is threats that are very constant and real. Nowadays most grave threats do not come from the well-known uninterested lone hacker in

high school nevertheless from classy organized crime organizations and, possibly, nation states. For instance, when Google in recent times got a lot of attention by announcing its servers had been subject to business spying, seemingly directed from Chinese informants, nobody supposed teenage hackers had anything to do with the attack.

Cyber security threats are basically put into three that are broad: (1) espionage (retrieving government, corporate or financial information); (2) attacks (rejection of service attacks, disruption of electrical networks, military command communications or air traffic controls); and (3) other wrongdoings (fraud, identity theft, and other corruptions). Attempted spying is a threat that is persistent; governmental, and military corporate records are continually subject to interruption. (Speed & Ellis, 2003) Alternatively, " attacks" include efforts not just to entrance and steal valuable data, but likewise to interfere and damage with computer systems. For instance, denial-of-service attacks are common, and goal to refute someone's aptitude to utilize a computer, server, or other forms of network resources. Research shows that Distributed denial-of-service (DDOS) assaults commonly encompass thousands of computers, which commonly overload a network resource like a server with requirements for evidence. Because of the requests, users that are legitimate are not able to have any kind access to the corporation's site. Further research does show that to analogize to the phone system, a Distributed denial-of-service would be similar to hundreds of individuals calling a corporation just to tie up the lines and keep genuine callers from getting through to seek help or place orders. With Distributed denial-of-service, instead of convincing hundreds or thousands of individuals

to go to the identical website, actors use a worm or virus that will infect a lot of computers, and then down the road give those computers that are compromised orders to demand information at the same time from the same site that is a target. Such a system of infested, controlled computers is frequently called a " botnet." Issuing spams some of the time works the same way; on the other hand, the botnet computers have orders to send emails that are unwanted rather than bombarding servers that are having requests.

Safeguarding the Open Internet

The Democratic congressional leadership, President Obama, and associates of the FCC have all recurrently stated their backing for network neutrality. (Speed & Ellis, 2003) Even though lobbying for the Presidency, Obama made a pledge the he would " not tolerate any bad conduct" in his support for bring neutrality to the network. (Ammori, 2010) In first part of 2009, Congress was able to tie incentive assets for broadband systems to the obligation of network impartiality circumstances in regards to receiving ISPs. (Kelly, 2002) Well ahead, in September of 2009, Obama's Federal Communications Commission Chairman, Julius Genachowski, projected a network impartiality law and endures to receive public comment on all features of the rule, as well as the security exclusion. (Nosek, 2012) Research shows that the motivation for a non-discrimination ideal is to make sure a level playing field among those that are speakers (Facebook, Twitter users, bloggers) and modernizers on the Internet. That is why, a proposed rule not allowing ISPs from differentiating among diverse websites and applications is key to the Federal Communications Commission’s proposed

network neutrality agenda. If an ISP (like Verizon) is able to discriminate against CNN. com and in favor of a competitor, like MSNBC. com, or against Skype and in favor of Yahoo Voice, then that ISP would be selecting the online losers and winners in innovation and speech a choice better left to personal consumers. Some experts of computers and hacking make the point that by influencing speech and the marketplace choices of users in this way, ISPs are able to obstruct robust speech and slow down financial innovation. (Treese, 2004)

However, when it comes to being beyond domestic rule, Secretary of State Clinton made some points that making sure an open Internet is now a being looked at as major foreign strategy goal. (Lee, 2012) In making the statement, Secretary Clinton started taking these a step further by criticizing governments all over the world for censoring blogs and social networks. Furthermore, censorship obstructs American companies' aptitude to contest justly in worldwide trade, something the control of Google results highpoints. (Kelly, 2002) Crafting a foreign policy to speak to censorship is harder than it looks. Countries could require ISPs to edit, could inspire such censorship, and, at any rate, allow ISPs extensive discretion in figuring out what to cut and what not to edit. Therefore, some characterize Chinese expurgation as being " outsourced" to ISPs determining what exactly to restrict. (Holden, 2003) From the viewpoint of democratic discussion, it does not matter much whether censorship derives from governments or from ISPs with adjacent relations to governments. Therefore, the United States will have to favor worldwide network neutrality. As stated by the Secretary's highest consultant on expending knowledge to further our diplomatic efforts, in

preferring global network neutrality, the United States more than likely would lose trustworthiness if it permitted its own ISPs nationally to affect with users' selections. (Ammori, 2010) So, domestic network neutrality progresses the foreign policy purposes.

Security Tokens

There are some online sites that are providing customers the ability to utilize a six-digit code which changes every 40-60 seconds randomly on a security token. However, the key on the security token have scientific computations incorporated and manipulate they do things like numbers based on the present time built into the method. This is saying that every thirty seconds there is only a certain likely collection of numbers which would be accurate in order to authenticate admission to the online account. With that said, the website that the person is logging into would become conscious of that devices' serial number and as a result would recognize the calculation and correct time built into the device to confirm that the number assumed is certainly one of the trickle of six-digit figures that would work in that assumed 40-60 second sequence. After the 40-60 seconds the computer will show a new unplanned six-digit number which will be able to log into the website.

Other industry features on the Internet

Research shows that organizations providing their products on the Internet might maybe suffer a channel battle with their existing suppliers. A corporation would need to work with its associates in order to come up with product prices that are fair. It could not be valuable to contend with a corporation's partners, since an organization could possibly want them at

another time in the future.

The territory likewise wants to be measured. The Internet is a worldwide open market and it could be hard to carry products to the customers. Clienteles start getting frustrated if they cannot buy the product directly and normally turn away from the buying.

Worldwide pricing likewise appears to be a factor that is important. Whereas businesses used to be able to attain dissimilar values for their products, they are pretty much destined to the fees that are usually cited on their Web pages. Investigation shows that it might be an answer to estimate a price after the buyer has entered some information concerning their wishes and nation of source.

Strain between Cyber security and Open Internet

On account of the potential need for ISPs to involve in application-exact directing of security threats, the tension among network neutrality and cyber security is well-documented in government rule and is also referenced in both the Cyber Policy Review Federal and Communications Commission network neutrality proposal.

So as to decide the tautness, authorities must be able to speak to both energetic threats and an absence of trust among key associates. These threats are dynamic for the reason that bad actors adopt new technologies rapidly, which results in a rapid fire technological arms race among bad and good actors. (Lee, 2012) At the same time, it is obvious that parties lack certain trust in each other that goes across almost every relationship. Initially, the public does not have trust in the government-an American tradition of sorts. For instance, groups have been complaining about cyber

security proposals that have the power to allow the President emergency power to elect and control specific systems in times of war or in case there is an emergency. (Nosek, 2012) The " warrantless wiretapping" disagreement, in which numerous have faith in that the Bush Administration ordered the National Security Agency to exceed then-current laws, could have caused public suspicion to rise for government cyber security efforts. (Speed & Ellis, 2003)

Also, ISPs have no trust in the government, because a lot of ISPs most of the time disfavor government regulatory orders, some of which could obstruct competence and decrease proceeds. ISPs likewise likely fear a public relations reaction for working too carefully with government-for instance, a lot of them have experienced some backlash over " warrantless wiretapping." (Nosek, 2012) In the same way, many civil liberties groups have no trust in the ISPs. This suspicion ascends partially from the Federal Communications Commission's decision in 2008 that the nation's major landline ISP, Mediacom, was not perfectly frank with the public and the agency in the Federal Communications Commission’s most significant network impartiality case to date. (Speed & Ellis, 2003) Furthermore, just this year, an additional ISP, RCN, acknowledged to appealing in similar behavior to Mediacom’s, having not revealed the situation until they were caught. (Lee, 2012) As a result, technology companies and consumer groups currently suspect ISPs of managing traffic in ways that are undisclosed. Not astonishingly, these same groups would possibly fear that ISPs could in secret use their " security" implements to handicap targeted requests.

We Have No Control over Security on the Internet

Research does show that Facebook frequently abuses the privacy of those that use the social site. Sites such as Google have are no longer supporting its popular RSS feeder. Even places like Apple are not even allowing all iPhone apps that are sexual or political. Microsoft could be collaborating with some administrations to spy on Skype calls, nonetheless we do not recognize which ones. Both LinkedIn and Twitter have lately suffered security openings that had some kind of an affect on the data of hundreds of thousands of those that are using it.

It is obvious that these are not traditional corporations, and we are not traditional clienteles. These are feudal lords, and we are their vassals, serfs and peasants. Power has moved in Informational Technology, in service of both cloud-service suppliers and closed-platform sellers. This power shift can have an effect on a lot of things, and it deeply affects security. Usually, computer security was the person’s concern. People actually started to buy their own firewalls, and antivirus software and any breaches were put on their carelessness. Many experts sort of refer to this as a kind of an irrational business model. Generally people suppose the services and products we purchase to be secure and safe, but in IT we accepted useless products and maintained a vast aftermarket for security (Speed & Ellis, 2003).

Conclusion

It is clear that security on the internet is a bigger issue than what most people actually even think about. On the policy side, it is apparent that we have some kind of an action plan. Basically as internet users, we will need to preserve circumvention—the capabilities to adjust our software, hardware, data records—legal and preserve the net neutrality. Actually, both of these

are important because each of them limit how much people will be able to take advantage of those that are big time internet users.

References:

Ammori, M. &. (2010). Security versus freedom" on the internet: Cybersecurity and net Neutrality1. The SAIS Review of International Affairs. The SAIS Review of International Affairs,, 30(2), 51-65.

Holden, G. (2003). Internet security: in easy steps. Barnes & Noble Books.

Kelly, G. (2002, Dec). Security, privacy, and confidentiality issues on the Internet. Retrieved from Journal of Medical Internet Research: http://www. ncbi. nlm. nih. gov/pmc/articles/PMC1761937/

Lee, M. &. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. Information Systems Frontiers, 14(2), 375-393.

Nosek, B. A. (2012). E-research: Ethics, security, design, and control in psychological research on the internet. The Journal of Social Issues,, 51(4), 161-176.

Speed, T., & Ellis, J. (2003). Internet Security: A Jumpstart for Systems Administrators and IT Managers. Digital Press.

Treese, W. (2004). The state of security on the internet. NetWorker,, 8(3), 13-15.