International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 4 –NOVEMBER 2014.

ETHICAL, LEGAL AND SOCIAL ISSUES IN E-BUSINESS

Dilleswara Rao M
Student (MBA-II[nd] Year), KBN College, Vijayawada, A.P., India
mdr.dhille@gmail.com

***Abstract*— Hacking is one of the most dangerous disease from which the global world is suffering from. This project concentrates on how the malicious attacks and the effects of hacking caused to our community. It provides complete picture and preventive measures so solve the problem of hacking. Different aspects of hacking are discussed over here. Today's generation is still lagging in solving the problem of hacking attacks and in taking out the preventive measures in solving this global problem which is increasing day by day. To solve this problem of hacking attacks sophisticated security tool are invented. That's why we should start to think about hacker's psychology as the main way to prevent and stop attacks by understanding their needs or desires. The invention of internet has solved many problems and brought many new things to this world like electronic commerce, easy access to vast stores of reference material, collaborative computing, email, and new avenues for advertising and information distribution, but at the same time it gave rise to the most dangerous problem called hacking. Critical Issues in Business Conduct addresses the legal, ethical, and social issues that will dominate business in the 1990s. From the impact of AIDS and problems of drug and alcohol in the workplace to financial accounting, employee rights, and sexual harassment, the book explores topical issues arising from the relationship between business organizations and their external constituencies as well as those that characterize relationships between firms and their own managers, employees, directors, and shareholders.**

Index Terms— Hackers, Internet, Governance, Expert regulation, Deliberative democracy

I. INTRODUCTION

Hacking means to "gain unauthorized access (to data in a computer)". Banks defines hacking as "something that boring mainframe computer operators did to improve performance and battle boredom." Here a bank focuses on boredom as the reason of hacking. Darlington believes hacking is not limited to accessing data or information but also includes an attack on the privacy of all people. Almost all different opinions agree on the illegality of hacking view of the hacker as a data lord, a barbarian who takes what he wants. Humane defines hacker as any person who performs illegal actions whether they were related to computer or not which means the usage of a device apart from its functionality.

"Hacking" is the word that shakes everyone whenever it is said or heard by someone. Everyone born in this world with attitude wants to be a Hacker. But it is not a job of a new born baby or an old grown lady. A Hacker needs a brilliant mind to hack anything. His skills should be so powerful that no other hacker can hack him. A Hacker doesn't need software to hack. There are many rules that he should learn to become an

II. HACKING WITH ETHICS

A.Hacking Websites If you possess the HTML & JAVA knowledge then u can even access password protected websites. To hack a Password Protected Websites just follow these steps: Open the website u want to hack. Provide wrong username password.(e.g. : Username - me and Password - ' or 1=1 --)An error occurred saying wrong username password. Now be prepared your work starts from here... Right click anywhere on that page go to view source. There u can see the html coding with JavaScript's. Before this login information copy your login the site in which you are. Then delete the java script from the above that validates your information in the server.(Do this very carefully, your success to hack the site depends upon this i.e. how efficiently u delete the JavaScript's that validate your account information)then look for...code ..: input name="password" type="password". Replace there instead of. See there if maxlength of password is less than 11 then increase it to 11(e.g.: if then write Just go to file => save as and save it anywhere within the hard disk with ext.html (e.g.: c: hack.htm).Close your webpage and go to the webpage u save in your hard disk (e.g. : c:hack.htm) Open it. U see that some changes in current page as compared to original One. Don't worry. Provide any username [e.g.: hacker] and password [e.g.:' or 1=1 --] Congrats! You have cracked the above website and entered into the account of 1st user saved in the server's database.Locally Stored Passwords

Most browsers, including Internet Explorer® and Netscape®, the AOL® client, and Windows® Dial-Up Connections allow you the option to store passwords. These passwords are stored on the local machine and (depending upon where and how it is stored) there is usually a method of

recovering these passwords. Storing any password locally is insecure and may allow the password to be recovered by anyone who has access to the local machine. While we are not currently aware of any program to recover locally stored AOL® passwords, we do not recommend that these are secure. Software does exist that can recover most of the other types of locally stored passwords. A Trojan is a program that is sent to a user that allows an attacker to control functions of the target computer, recover information from the target or to delete or damage files on the target. The name Trojan is given because the program will usually come attached to some other program or file that entices you to run it. There are a wide variety of Trojans any number of which can be programmed to capture passwords as they are typed and to email or transmit them to a third party. To protect yourself against Trojans, you should never execute or download software or files that are not from a trusted source. It is critical that anyone working on internet use a virus protection program (which should catch most Trojans.) Note that since a Trojan requires the password to be typed or stored in order to be recovered, this is not an effective way to recover your own password. It could explain, however, how someone could lose their password to a hacker. Sending someone a Trojan program is certainly illegal and we do not recommend or condone this activity. A Trojan is unlikely to be effective in recovering a particular account password since it requires the target to install it. However, hackers will often bulk mail Trojans to thousands of people in the hope that a small percentage will get caught. D. Key logger

A key logger is a program or piece of hardware that records all keyboard keystrokes to an encrypted file which can then be read later. Based on the order of the keystrokes, it is usually easy to identify the password(s) from the file later. Like the Trojan, this also requires that someone actually type the password. Key loggers come in two types: hardware and software. A hardware key logger can be fitted between the keyboard cable and the computer and can be activated with a few keystrokes. It is then left in place until after the password that you are looking to recover is typed. Later it is removed and the file of keystrokes is examined for the password. A hardware key logger is un deductable by antivirus software.

A software key logger is installed on a system and effectively has the same function, however, it is a little bit more complex to use since it must be installed to run stealthily to be effective. A key logger could be used to steal a password from someone who is using an office computer or sharing a computer. It is possible that installing and using such a device or piece of software could be illegal depending upon whether the target has a presumption of privacy when using the computer on which the key logger is installed It is possible to impersonate a program on a computer by launching windows that look like something else. For instance, let's say you login to the MSN® service and visit a website (in this case a hostile website.) It would be possible for this website to pop-up some windows that look like something else. They could look almost identical to windows that an inexperienced user might expect from his local computer. The user could be fooled into submitting information to the hostile website. For instance, consider the effect of seeing the following series of windows If these could trick you into entering your password, then you could end-up sending your password to the attacker. Windows such as these could be created to mirror virtually any program or series of actions. Your browser will likely identify your operating system and your IP address might identify your ISP. Therefore, a hostile website could target you with a series of screen shots that look exactly as they should on your system. The key is that the screen shots are not coming from your system, but are coming from the hostile website. First, creating such a hostile website is probably fraudulent and illegal. We do not recommend or condone this activity. To protect yourself against this type of attack, make sure to configure your browser for high security and enable warnings for any code that is executed on your system. Sniffing If two people do not share the same computer, but do share the same network, it may be possible for one to sniff the others' packets as they sign-on. The traffic between your computer and the internet site you are accessing may be able to be recorded and decrypted or "played-back." This is not a simple attack to execute, but is possible if two people are close to one another and share a hub. Again, this is likely to be illegal and we do not condone this activity

Social Engineering

Social engineering is the name given to the art of attacking the person, rather than the computer or system. The basic principle is that many people can be talked into giving someone else their id and password if they think it is someone that they can trust. For instance, I might call someone and say I was from AOL and that I was finally getting around to responding to their technical support question. I would then ask you to describe the problem that you are having and tell you that we have a solution. However, I just need to verify the account. Can you give me the username and password again? A surprising number of people would fall for this obvious scam. There is no limit as to how elaborate this can be. The more information that is given by the caller, the more realistic or believable the call is. Again, never give your password to anyone. No legitimate customer service representative will ask for this information. These are the basic methods that we are aware of for hacking an AOL®, Yahoo®, Hotmail® or any other dial-up or on-line password. Hopefully this will answer some questions and help you protect yourself against this attack learn about computers - in as much detail as you can-now most people will disagree with this but the first thing you should do is learn HTML this way you will know how to make decent websites. you may wonder why? Because hacking is knowing everything about a computer an using that knowledge to get what you want. Now after you have done this you can start on this list of things to do.

Code of Ethics

Learn about hardware - basically how your computer works. Learn about different types of software. Learn DOS.(learn everything possible) Learn how to make a few batch files. Port scanning. (download blues port scanner if it's your first time) Learn about hardware - basically how your computer works. Learn about different types of software. Learn DOS.(learn everything possible) Learn how to make a few batch files.

Port scanning. (download blues port scanner if it's your first time) Learn a few programming languages HTML,C++,Python, Perl recommend learning html as your first Lang) How to secure yourself (proxy, hiding ip etc) FTP TCP/Ip , UDP , DHCP

III. PRESUMPTION IN E-BUSINESS

The Internet is a growing and a continually evolving creature that will live on in perpetuity. As such, it would be wise to ponder the various e business legal and Internet marketing ethical issues of both B2B and B2C business practices online. Whatever is written and published online today will likely be there tomorrow and possibly be recoverable forever. Imagine the billions upon billions of text information in web pages, publications, and books that are and will be stored for a long time to come. There is even a site where you can go way back in time to check out archives of other websites and view pages that were created at the beginning of their infancy. Additionally, old videos, films, movies, and audio in various applications formats are also viewable. With text messaging, wireless web mail, picture uploading, video recordings, and even video conferencing from cell phones and other personal communication devices with built in microphones and cameras, the Internet will be affecting more lives than ever before. Security and privacy concerns, along with ebusiness regulatory issues will become more prevalent. It will become more difficult to figure out who you can trust online, which websites are safe to visit, along with all the unethical, illegal, Internet marketing schemes, search engine optimization, search engine marketing, and online advertising frauds and all types of e- business email scams to contend with. Applying good ethical standards to the online world is a direct reflection of your business online. Ethics affects all aspects of your business. It affects first and foremost your company's brand image and subsequently how sales, marketing, and advertising principles are applied to the task of making your company profitable for the long haul. Ethics affects your employees, and how they represent your company online, on the phone, in person, and all types of customer service and customer relations when dealing with buyers, engineers, sales leads, and potential customers.

IV. THREATS IN E-BUSINESS

E-business Security also has some main issues. They are interception of data, redirection of data, identification of parties, exploitable program errors, and being the weakest point in security. When administrating a secure Ebusiness site, it is important to remember that you are part of a link of systems. If you're security is weak, it may be possible that you are allowing criminals access to information they may not have had access to. This leads to ethical issues where weak security on your system led to dire consequences for other people or companies. Compare security issues over the Internet compared to real-life. Is it right to be protective of information over the Internet when people are not protecting that same information normally? Is it ethical to deliver different punishments to criminals who steal information over the Internet compared to those who steal information personally?

A) The Threats Posed to E-business Servers E-business tends to be at a higher echelon for risk and attacks. This is so because according to our definition, E-business is the transaction of goods and services; and the payment for those goods and services over the Internet. Therefore, the physical place where all of these transactions occur is at the Server level. The server can be viewed as the central repository for your "E-business Place of Business "which consists of the actual website which displays your products and services, the customer database, and the payment mechanism]. If there are any attacks to this server, in one blow, there is the potential you could lose everything. The intent is to garner personal information from people for the sheer purposes of exploitation (such obtaining Credit Card and Bank Account information; Phishing schemes, obtaining usernames and passwords, etc.).

With the latter, anything related to the Internet can cause problems. This can be anything from a network not configured properly to data packets being lost, especially in a wireless access environment. Even poorly written programming code upon which your ECommerce site was developed can be very susceptible to threats. Most E-business Servers utilize a Windows Operating System (such as Windows 2000 and 2003 Server), a Web Server Software to host the ECommerce Site (such as Internet Information Services, or IIS), and a database (such as Access 2000 or SQL Server 2000) which contains your customer information and transaction history. These platforms have had various security flaws associated with them, which has made them wide open to threats and attacks. As a result, there has been a move in the business community to adopt more robust and secure platforms. A prime example of this is the use of Linux as the operating system, Apache as the Web Server Software, and either PostGRESql or My SQL as the database (these are database languages created from the Structured Query Language, or SQL). These latter platforms will be explored in much more detail in subsequent articles. We will now

examine the various threats and risks that are posed to E-business servers.

V. REFERENCES

[1] 1.E .S Raymond, The New Hacker's Dictionary, MIT Press, Cambridge, A (1991).

[2] S. Garfunkel, Database Nation, O'Reilly &Associates, Cambridge, MA (2000).

[3] The first use of the term "ethical hackers" appears to have been in an interview with Johan Patrick of IBM by Gary An then that appeared in a June 1995 issue of computer world.

[4] P .A. Karger and R. R. Schell ,Multics Security Evaluation: Vulnerability Anaiysis,ESD-TR – 74193.Vol.2, Headquarters Electronic Systems Division,Hanscom Air Force Base, MA (June 1974).