A Brief Introduction To The Tools And Techniques Of Cyber Crimes And Its Prevention

Sara Qayyum[1] , Nadia Noreen[2] , Kokab Saeed[3] , Alam Zeb Khan[4] , Dr.Suhail Shehzad[5] , Hidayat Ur Rehman[6] , Dr.Bahadur Ali[7] , Saqib Javid[8] , Kamran Khan[9] , Aliya Mahnoor[10]

[1,2,3,]Assistant Professor Department of Law Hazara University Mansehra

[4]Assistant Professor School of Law, Quaid I Azam University Islamabad

[5]Professor,Law College University of Peshawar

[6]Assistant Professor Department of Law AWKUM

[7]Lecturer Department of Law University of Malakand

[8]Lecturer Department of Law Hazara University Mansehra

[9]Research Associate, Department of Law Hazara University Mansehra

[10]LLB Scholar

Abstract

Cyber Crimes and its prevention has become a global issue. The ratio of cyber crimes is increasing day by day and the law enforcement agencies find it difficult to control it. The reason is that the cyber criminals use highly technical tools and techniques while the commit the offences. Furthermore, laws related to the prevention of cyber crimes are not up to date, consequently, the criminal take advantage of the lacunas in the system. The research article, first elaborate the various types of cyber crimes the tools adopted for its commission and then recommends suggestion to cope with it.

Key Words: Cyber Crimes, Internet, Spam, Data, Theft, Pishing, Hacking

Introduction

Cyber Crimes make use of various tools and techniques and many of these tools are used for the commission of the cyber crimes and are installed on the victim's systems through - exploitation of the vulnerabilities in the systems / networks or by surreptitiously gaining access to the victim's systems which may include physical access or by making use of the intermediary systems or by deceiving the victim to allow access to his system or by gathering the victim information.[1] Before the article proceeds to suggest that how cyber crimes could be prevented, it is necessary to throw a glance on the various terminologies of the cyber crimes which are elaborated as below.

Buffer overflow: The condition when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

Cracking: Cracking is breaking into someone else's computer system, often on a network; bypassing passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this either for profit, or maliciously, or for some altruistic purpose or cause.

Data Didling: Involves altering the raw data just before a computer processes it and then changing it back after processing is completed.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. **Phishing:** Using spoof E-mails or directing the people to fake web sites to deceive them into divulging personal financial details so that criminals can access their accounts.

Rootkit: A set of tools that enables continued privileged access to a computer, while actively hiding its presence from the administrator. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. [2]

Salami Attack: A programmed attack which is implemented in small (meant to be unnoticeable) increments. This attack involves making alteration so insignificant that it is easily concealed and would go completely unnoticed. Attacks are used for commission of financial crimes.

Sniffer: A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted

[1] https://www.academia.edu/resource/work/31750862

[2] http://www.unodc.org/documents/organizedcrime/unodc_ccpcj_eg.4_2013/cybercrime_study_210213.pdfalmost anywhere.

Social Engineering: A hacker term which involves non-technical intrusion for deceiving or manipulating unwitting people into giving out information about a network or how to access it.

Spoofing: Refers to a situation in which the incoming information from an attacker is masqueraded as one that appears to come from a trusted source to the recipient or to the recipient network. Often the messages from the fraudster appearing to be from a genuine source (like bank), seeks personally identifiable information to perpetrate fraud on the victim.

Spyware: It is a type of malware that is secretly or surreptitiously installed into an information system to gather information on individuals or organisations without their knowledge; a type of malicious code.

Steganography: The art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message An image file may contain hidden messages between terror groups, which will be known only to the intended recipient and the sender

Trojan: A malicious program that masquerades as a benign application andcan take complete control of the victim’s computer system.

Virus: A self-replicating program that runs and spreads by modifying other programs or files.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Zombie: A program that is installed on a system to cause it to attack other systems.

Types of Cybercrime

Following are the types of cyber crimes usually committed in Khyber Pakhtunkhwa, Pakistan.

- Hacking
- Phishind and scamming
- Porngrphy
- Data theft

Hacking

Hacking is an illegal access to someone’s computer. That computer does not belong to the person who is hacking it. In today’s modern time it is very important to find the solution to this serious problem. In order to solve this issue we follow a game theory perspective. Suppose there are two players in this game. The computer which is at stake is person X and the person who wants to gain access to person Xs computer is person Y.

Both people will try to win this game. Person X will try to protect his computer and person Y will try to attack person Xs computer. In today's modern time every person is person X. But if person X wants to be smart he should think like a hacker. The hacker, person Y keeps an eye on the victim's actions and person X, the victim will try to protect himself to lower the risks. There are many options for a victim to secure himself. For example he can do a security assessment. He can install security solutions. He can also take steps to protect the machine physically. By summing up, we will look that there are three possible threats that person X can face.

Insiders

There is a greater threat from insiders than outsiders. There are many reasons why they are interested in stealing our data. They may do it because they want to work from home or to save the data for future use. They can also make a plan to complain against the company for which they need to steal the data. Even if we take strong prevention methods, the main point of ingress for the hackers will continue to be the members of staff who are not loyal because of greed or ignorance etc. A company should be careful when giving database access to the employees because every insider can be a risk.

Social Engineering

The hacker wants to gain access to the IP address, database, usernames with email IDs,s and the security methods used in an organisation. Now it is obvious that the company will not reveal their secrets that are why the hacker will target an insider. The process of social engineering involves persuading an insider to leak the data which is needed. This can be carried out by over communications media or face to face etc. In social engineering no special software is needed, only clever words are enough. The hackers usually target the junior staff members who are not familiar with the risks and with the most of the company employees. Each company can create a human firewall in which they can train their employees on how to defend themselves from social engineering.

Outsiders

Any individual who is not provided access to the device by the owner but he tries to get illegitimate access is called an outsider.

- **Wireless Networking**

Wi-Fi attracts the hackers who either want to connect it freely or wants to steal the data. Unprotected Wi-Fi is very easy for a hacker because any device with wireless connectivity will display the available networks and there will be an option to connect to any of them. Then they can use a program that searches for WAP and helps the 34 hackers to choose the fastest connection with the best signals. Therefore the Wi-Fi connections should be protected. Bluetooth can also be used to steal Wi-Fi, therefore when Bluetooth is not in use it should be turned-off.

Firewall

Firewall is a necessary tool for security. It is an electronic filter that blocks communications over the internet according to their source, direction or port number. The firewall can only protect from outsiders.

Insiders and Outsiders

In order to reduce the risk of hacking the person X should maintain a backup. It is a copy of a person database.
The data in any form should be encrypted as well. For added security the person can add USB sticks and portable hard disk drives.
In addition the passwords also need to protect.

One-Time Passwords

These passwords expire after each use. The new list of passwords are secretly issued by a secure email.

Duress Passwords

In panic situations the user enters the panic password that sends signals to the system that the password is entered under the panic. Duress passwords can be helpful in many cases.

Denial Of Service Attacks

Denial of service attacks require the hacker to use the facilities which are publicly available to attack the computer and make the computer temporarily unavailable to its legitimate users. The hacker is not worried about overcoming security barriers such as passwords and firewalls. Denial of service attacks to exceed the limit to the extent that the system will not be able to proceed the request which results in system crash. The attack source should have a larger server than the victim so that it will be able to send the sufficient volume of data.

Defacement

When a hacker does unauthorized alteration of a content of a website or any other media it is called defacement. The target of defacement is the website so for the security of the website the steps should be taken. At the owners premise the website servers can be placed. Type of file users should be restricted by the website owners as a safety precaution because any file may contain poisonous script. A security certificate should also be used when anyone is passing personal information between the website and web server. Security software should also be downloaded to do penetration tests.

Understanding Phishing, scamming and Spam

Spam

The curse of irrelevant bulk emails is known as spam. Irrelevant and bulk emails separately do not count as spam. Spam is usually ignored. Average rise of email accounts owned per person is from 1.7 to 1.9. The phishers and scammers will have a larger pool of targets with this increase in number. Average number of spam per person increases from 12 in 2015 to 19 by 2019. All are not sent by the humans behind the computers.

How it's Done Phishing?

Phishing like fishing is the setting of automated bait to attract the target to reveal its identity and sensitive information. The target gets an email with a look of a legitimate business or organisation to reveal personal information. It includes passwords, credit card numbers or usernames i.e any information that can be used to steal the money. The most common questions are that the company has lost your information or it is required to confirm the information again so the service can be resumed or otherwise the account will be expired. Many people do not give personal information but many fall for such scams because the frame of email looks legit. Some emails also have spyware in which the data of the user is collected in the real website and then sent back to the phisher. Phishing is where the money is therefore their targets are banks etc.

Spear-Phishing Attacks

It is a more targeted attack and the victim is not a random person. The phisher chooses his target intentionally by studying them. The address of the sender is usually from where the phishes get regular emails. For this purpose the social networking sites become the best source for knowing about the target's interest and his hobbies and lifestyle etc. All this information is used to send more personalised emails. A man was sentenced to imprisonment in 2013 for stealing from UK students. For the phishing purpose the students were sent a fake link in which they were asked to update their student loan account.

Free Advertisement

Spamming is a very attractive form of advertisement. Majority of people would have given their phone numbers or email IDs while shopping. The companies collect this data and sell them to the buyers. A buyer can be from a local business trying to sell their product or they can be a scammer trying to loot money. When the information is leaked then it is impossible to stop the information from spreading. To avoid spamming many people have made multiple email accounts. One app Unroll.me blocks the emails that send the greatest number of spam and it has released a list of companies that release such emails [3]

How to Protect Against Spam and Phishing?

- It is not possible to eradicate it completely.
- Do not open any suspicious email and delete it immediately.
- Use spam filtering and blocking softwares.
- Use an email address that has numbers and symbols in them
- One should have disposable account when there is a time to provide email address.

Pornography

The first ever pornographic movie production started in 1895 by two persons, Eugene Pirou and Albert Kirchner. In today's world there are indeed countless pornographic sites, magazines, nude snaps etc. Pornography is considered in some parts of the world as a taboo. In some jurisdiction around the world it is a criminal offence. According to a survey conducted by Google, Pakistan, Egypt, Vietnam, Iran, Morocco, India, Turkey, Philippines, and Poland are amongst the top porn watching countries (Staff, 2015). Child sex is a very big industry and it is expanding at a very high rate, it is a very alarming situation for the world. As per reports of different international organizations working in the field of child sex, many young girls are sexually exploited and in different parts of the world, they are forced to enter the child sex industry. Some of these young girls are sold to the highest bidder; some are used for smuggling purposes. Some countries in Europe like Nederland, their economy is dependent upon sex and it includes up to some extent child sex too. This industry contributes a lot to their countries GDP.

The people or groups involved in running a child sex industry, become very rich in a very short span of time. The sexual exploitation of young girls is indeed a very profitable business for such bad and horrific people. Ukraine is considered to be a very big market of the child pornography. A very large of it is even made there. It won't be wrong to say that Ukraine is kind of a central hub of child pornography in the modern world. Girls at very young age are sexually exploited and their nude and explicit content is shared on different pornographic sites. The international agencies have failed to control or limit such shameful act.

Data Theft

Data theft is the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information. Data theft is increasingly a problem for individual computer users, as well as big corporate firms. The following categories are most common in data theft cases.

- **E-commerce:** You should make sure that your data is safe from prying eyes when you sell or buy things on the Web. Carelessness can lead to leaking your private account information.
- **Password cracking**: Intruders can access your machine and get valuable data if it is not password-protected or its password can be easily decoded (weak password).

- **Eavesdropping:** Data sent on insecure lines can be wiretapped and recorded. If no encryption mechanism is used, there is a good chance of losing your password and other private information to the eavesdropper.
- **Laptop theft**: Increasingly incidents of laptop theft from corporate firms occur with the valuable information stored in the laptop being sold to competitors. Carelessness and lack of laptop data encryption can lead to major losses for the firm.

Effective Prevention of Cyber Crimes____ How?

The perspective of business is changing by using technologies of mobile and electronic commerce and many other things. As business organization are planning to use these technologies to share and conduct their information on the internet. Therefore the requirement of high level security is needed so there will be less chances of transaction failure. As cyber security is not limited to protect the local information so the cyber security role cannot be ignored in the current situation. It is really essential to make the internet secure to protect the user of internet from cybercrime attacks. The study conducted a survey in different cities of Khyber Pakhtunkhwa and we get 200+ responses. After getting the responses we converted the data into format suitable. Trend analysis was also made with the help of frequency distribution as well as with standard deviation to study the correlation between genders. In response to this we estimated how serious an issue is considered and how the security measures are taken. As a female I checked the correlation between women and victimization and the result was that correlation between women and victimization is stronger than the correlation between man and victimization. This means that the chances of female victimization are higher than the men victimization.

Cybercrime against Individuals

A major problem of cybercrime against individual can take place towards different types of people such as cybercrime against children, cybercrime against consumers and cybercrime against normal users. It is clear that cybercrime against children is the most significant issue which should be focused on. One of the main areas of cybercrime is child pornography, which is the documented sexual abuse of children, however this excludes pseudo-photographs or computer generated items such as images, drawing, cartoons and painting that the internet has authorized to child pornography by offering offenders many ways of swapping information without restraint and giving them a chance of learning and improving skills illegally. Thus, under a high activity by predators of finding open contacts with young victims such as teenagers, a rise in the number of children who use the internet and spread child pornography that cause a serious threat to the safety of children. There are several ways that predators used to meet their young victims in public place and one of the common ways is chartrooms

Cybercrime against organizations

The second problem of cybercrime is one that is extremely threatening to organisations such as business and political websites, to name but a few. It is quite common that cybercriminals are focused on attacking one particular sector which is commercial websites such as the shopping websites and banks. Cybercrimes against commercial websites can be accrued in several ways, however, in cyberspace there is one common activity between cybercriminals which is piracy such as downloading music, films and games illegally and stealing information or any substances that are private or not made freely accessible. In contrast, pirated software programs often cost from several hundred to several thousand dollars. Thus, economically, one act of software piracy is several times more "serious" than victimization by a petty thief or robber".

Suggested Solution of cybercrime against organization (commercial website)

Organizations and companies come under cybercrime attacks in every business activity in cyberspace; therefore, some solutions can be suggested that may help to protect business websites. Companies should develop and secure their websites by providing anti-piracy software which could possibly help to reduce the risk of cybercrime and their activities. In addition, businesses ought to hire some people who are sophisticated and experts in computer security to supervise their content and materials which give a secure environment in cyberspace. Moreover, companies should be advised to join some organization and the international cooperation groups in order to eliminate piracy as well as establish an international law in cyberspace, which punishes anyone who commits action of cybercrime.

Enforcement of Cyber Security Laws

Pakistan is among those countries that have passed cyber laws for protecting and promoting of the electronic transaction. The people committing cybercrimes should be dealt with iron hands and the laws should be amended accordingly. This will not only prevent the fast rate of cybercrime but will also motivate the victims to report more about the cybercrimes. It seems that the laws that are meant to protect the cyber community from intended crimes; are not sufficient to safeguard the non – commercials problems especially the use of internet for spreading of extremist ideologies in Pakistan. The extremists performed unlawful activities on the social media worldwide and Pakistan in particular. These activities not only disturb the autonomy and trustworthiness of individuals but institutions as well. It requires exhaustive policies to cope with cyber terrorism and cyber extremism. These laws could be synchronized with global community in combating terrorism rather cyber terrorism. Some other recommendations are to extend the development of specialist police and forensic computing resources. Support the international Computer Emergency Response Team (CERT) community, including through funding, as the most likely means by which a large-scale Internet problem can be averted or mitigated. Fund research into such areas as: Strengthened Internet protocols, Risk Analysis, Contingency Planning and Disaster Propagation Analysis, Human Factors in the use of computer systems, Security Economics.

Recommendations for Attitudes to Cybercrime

There are also some possible solutions around dealing with cybercrime and attitudes to

it:

- .There should be government developed awareness programmes, including TV, radio, internet ads, etc. on the impact of cybercrime which could include testimonials from victims and short case studies that outline some high profile cases.
- .Parents need to be made aware of how easily their children can become script kiddies, and generally parents need to educate their children that their activities online have real consequences for real people. E.g. similar to cyber bullying campaigns.
- As the cyber security experts, an increased onus on the owner of public systems and infrastructures to ensure their security could reduce the general levels of vulnerability to cybercrime. E.g. if organisations were also punished (in addition to the attacker being punished) for failing to secure their systems, they might be more proactive about patching which would make it less likely that script kiddies would be able to find vulnerable targets.
- .Alternative penalties could be introduced for cybercrime, such as banning them from using computers, or making them work for free for the victims of their crimes.

By Using Strong Passwords: Maintaining different password and username combinations for each of the accounts and withstand the desire to write them down. Weak passwords can be easily broken. The following password combinations can make password more prone to hacking:

- Using keyboard patterns for passwords. e.g. – wrtdghu
- Using very easy combinations. e.g. – sana1999, jan2000
- Using Default passwords. e.g. – Hello123, Madhu123
- Keeping the password the same as the username.

Keep social media private: Be sure that your social networking profiles (Facebook, Twitter, YouTube, etc.) are set to be private. Once be sure to check your security settings. Be careful with the information that you post online. Once if you put something on the Internet and it is there forever.

Protect your storage data: Protect your data by using encryption for your important diplomatic files such as related to financial and taxes.

Protecting your identity online: We have to be very alert when we are providing personal information online. You must be cautious when giving out personal ids such as your name, address, phone number, and financial information on the Internet. Be sure to make that websites are secure when you are making online purchases, etc. This includes allowing your privacy settings when you are using social networking sites.

Keep changing passwords frequently: When it comes to password, don’t stick to one password. You can change your password frequently so that it may be difficult for the hackers to access the password and the stored data.

Securing your Phones: Many people are not knowing that their mobile devices are also unsafe for malicious software, such as computer viruses and hackers. Make sure that you download applications only from trusted sources. Don't download the software /applications from unknown sources. It is also pivotal that you should keep your operating system up-to-date. Be sure to install the anti-virus software and to use a secure lock screen as well. Otherwise, anybody can retrieve all your personal information on your phone if you lost it. Hackers can track your every movement by installing malicious software through your GPS.

Call the right person for help: Try not to be nervous if you are a victim. If you come across illegal online content such as child exploitation or if you think it's a cyber-crime or identity theft or a commercial scam, just like any other crime report this to your local police. There are so many websites to get help on cyber-crime.

Protect your computer with security software: There are many types of security software that are necessary for basic online security. Security software includes firewall and antivirus software. A firewall is normally your computer's first line of security. It controls that who, what and where is the communication is going on the internet. So, it's better to install security software which is from trusted sources to protect your computer.

How Secure Your Smart Phones?

- Always secure your smartphone with a strong password
- Ensure that your device locks itself automatically
- Install security software
- Only download apps from approved sources
- Check your apps permissions
- Dont miss operating system updates
- Be wary of any links you receive via email or text message
- Turn off automatic Wi-Fi connection

How to Secure Your Online Banking?

- Never use same PIN CODE for multiple bank accounts
- Never use unprotected PCs at cybercafes for internet banking
- Never keep your pin code and cards together
- Never leave the PC unattended when using internet banking in a publicplace

- Register for Mobile SMS, Email Transaction Alerts
- Never reply to emails asking for your password or pin code
- Visit banks website by typing the URL in the address bar
- Log off and close your browser when you are done using internet banking
- When using ATM always conceal keypad before entering pin code
- Before using ATM, make sure that there is no extra device installed in the surroundings

How to Secure Your Facebook?

- Use extra security features to access account (security code, Login alert etc)
- Use login notification alert
- Allow specific individuals to view your contents (Videos, Photos and Friends etc.)
- Control who can contact you
- Block your profile from search engines

How Secure Your Wi-Fi?

- Change Default Administrator Passwords and Usernames of the Wi-Fi Router
- Use complex password and change Password after regular intervals
- Position the Router or Access Point Safely
- Turn off the Network / Wi-Fi routers if it is not in use

How to Secure Your Browsing?

- What you put online will always remain there
- Never trust any free online content
- Dont provide personal information online to get something free
- Don’t click on links inside e-mails or message

Conclusion

It is shown that in one way or the other, cybercrimes are silently present and pose a threat to the developed and developing countries. The instances of cybercrimes are not reported rather discussed socially; on the other hand the perpetrators are invisible under the cyber world. This is a crime

Beyond the border so it is hard to bring the cyber criminal under justice system. The laws needed to be modified and cooperation with international community in this regard should be established. It is also hard to obtain facts from internet or computer crime that are needed to prove someone a culprit in a court of justice. Computer forensic is still a new area and mostly the countries are lacking the expertise and literature. KPK should adopt the proper laws and procedures of anti cyber crimes effectively. On the other hand it has been proven that it is the responsibility of the individual to protect his/her own Internet connection. It could therefore be suggested that Governments and local authorities including Police and Education Services should work more closely with the Internet Service Providers to protect minors on the Internet. Despite all the developments in the domain of Child Protection Software, young people will always find a way of avoiding a protective firewall. Therefore education would serve an important role in protecting children. Furthermore if the culprits are identified law enforcers could punish and remove the criminals' access to the internet.

References

https://www.satp.org/potential-threat/cyber-crimes/pakistan-khyberpakhtunkhwa-khyberpakhtunkhwa#

https://www.geeksforgeeks.org/cybercrime-causes-and-measures-to-prevent-it/

https://www.loc.gov/law/foreign-news/article/pakistan-national-assembly-passes-new-cybercrime-law/

http://dx.doi.org/10.31703/gpr.2019(IV-II).02

https://www.academia.edu/resource/work/31750862

http://www.unodc.org/documents/organizedcrime/unodc_ccpcj_eg.4_2013/cybercrime_study_210213.pdf

https://www.academia.edu/resource/work/44258539

http://www.nr3c.gov.pk/ctips.html