International Journal of Science and Healthcare Research
Vol.4; Issue: 3; July-Sept. 2019
Website: www.ijshr.com
Review Article *ISSN: 2455-7587*

Beware of Cyber Crime with Awareness - A Review

Dr. Farzana Begum

Assistant Professor, College of Nursing, Rajendra Institute of Medical Sciences, Ranchi, Jharkhand

ABSTRACT

Objective: To spread awareness regarding measures to be taken in order to combat cybercrime.
Methods: Fifteen articles were retrieved from electronic databases that met the selection criteria with papers discussed in relation to various forms of cybercrime and measures to prevent and handle such things.
Results: Awareness about various forms of cybercrime and measures to prevent and tackle such issues is the only way to combat cybercrime.
Conclusions: Cybercrime continues to evolve, with new threats every year. Abstinence from internet use is not the solution. Instead recognizing cybercrime and understanding the prevention and management strategy are important.

Keywords: Beware, Cyber, Crime, Awareness

INTRODUCTION

The current world is digital world. To cope with the digitalized world, people are forced to use internet for all types of services. On the other hand digitalization also brought unprecedented threats, cybercrime.

Cybercrime is a crime attempted through a computer for crime like hacking, spamming, phishing etc. Cybercriminals or Hackers use the internet to hack user's personal computers, smart phone data, and personal details from social media, business secrets, national secrets etc.[1]

Cybercrime is growing rapidly and many people have become victims. Various categories of harassment take place in cyberspace.[2]

Cybercrime, being a burning issue across the globe, many countries have implemented laws and other regulatory mechanisms in an attempt to minimize cybercrime.[2] The government working hard to fight against this.[3]

Body of the content:

Definition of cybercrime

Any crime that takes place online referred as cybercrime. Cybercrime can range from security breaches to identity theft.[4]

Forms of cybercrime[1,2,3]

Cybercrime may be broadly classified into the following groups.

1. Crime against Individuals: Person/Property
   Against Individuals Person: - Harassment via electronic mails, dissemination of obscene material, cyber-stalking, defamation and fraud etc.
   Against Individual Property: - Computer vandalism, transmission of virus, control over computer system, intellectual property thefts etc.
2. Crime against Organization: Government/Firm/Company/Group of Individuals
   Against Organization: - Unauthorized access / control over computer system, distribution of Pirate software.

3. Crime against Society
Against Society: - Pornography, sale of illegal articles, trafficking, forgery, online gambling.

Terminology

- Phishing: using fake email messages to get personal information from internet users;

- Misusing personal information (identity theft): - accessing data about a person's bank account, credit cards, debit card and other sensitive information to buy things online in the victim's name.
- Hacking:- personal or sensitive information can be accessed. The criminal uses a variety of software to crack a person's computer and the person may not be aware that his computer has been accessed from a remote location.
- Spreading hate and terrorism;
- Distributing pornography: - internet is being highly used to abuse anybody sexually worldwide.
- Piracy or Theft: - occurs when a person violates copyrights and downloads music, movies, games, and software.
- Computer Vandalism: a type of malicious behavior, involves creation of malicious programs to perform harmful tasks such as erasing hard drive data or extracting login credentials.
- Malicious Software: Internet-based programs used to gain access to a system to steal sensitive information or damaging to software present in the system.

Causes of Cybercrime[1]

- Easy access –many possibilities of breach due to the complex technology.
- Store data in comparatively small space – makes easier to steal data and use them for own profit.
- Complex – The computers run on operating systems those are programmed of millions of codes. The human mind is imperfect, leads to mistakes at any stage and become prey for cybercriminals.
- Loss of evidence – Data related to the crime can be easily destroyed. Loss of evidence has become a very common problem that paralyzes the system behind the investigation.

Combating cybercrime[1,2,5,6,7]

To combat cybercrime, establishment of multidimensional public-private collaborations needed between law enforcement agencies, information technology industry, information security organizations, internet companies, and financial institutions.

- Cybercrime can be particularly difficult to investigate and prosecute as it often crosses legal and even international boundaries. However an investigation tends to start with an IP Address trace, though that is not sufficient to solve a case.
- Enforcement of strong law and setting high penalties.
- Government of India under National Mission for the safety of women facilitate victims to report cybercrime online through cybercrime reporting portal.
- Law enforcement agency (local police department) has an obligation to assist the victims.
- The Internet Crime Complaint Center (IC3) thoroughly reviews and evaluates the complaints and refers to the appropriate federal, state, local or international law enforcement/ regulatory agency that has jurisdiction over the matter. IC3 is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center (funded, in part, by the Department of Justice's Bureau of Justice Assistance).
- Federal Trade Commission (FTC) is a secure online database, used by civil and criminal law enforcement authorities worldwide to detect patterns of wrong-doing, leading to investigations and prosecutions. It does not resolve complaints but operate the Consumer Sentinel and provides resources for victims, businesses and law enforcement.
- Local victim services provider: these providers offer information, emotional support and advocacy as needed

- Collect and keep evidence to provide them for investigation. The evidences may be a cancelled check, certified or other mail receipts, chat room text, credit card receipts, received envelopes, social media messages, money order receipts, pamphlets or brochures, phone bills, printed or preferably electronic copies of emails/web pages etc.
- Complete Termination of Online Session: - Closing the browser window or typing in a new website address without log in gout may give others a chance of gaining access to account information. Always terminate online session by clicking on the "Log out or Sign Out" button. Avoid using the option of "remember" your username and password information.
- Create Backup of Important Data: - Backup of all the important files whether personal or professional should be created. Getting used to back up files regularly is the first step towards security of personal computer. Protect data by using encryption for most sensitive files such as financial records and tax returns.
- Use Security Programs: - If system does not have data protection software to protect online, then buy internet security program for the computer. Nowadays, almost all new computer systems come with some kind of security programs installed.
- Use Strong Passwords: Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc. Try creating a password that consists of a combination of letters (both upper and lower case), numbers and special characters. Password should be changed regularly. Do not share password with others.
- Be social media savvy: Be sure to keep social networking profiles (Face book, Twitter, YouTube, etc.) are set to private. Beware of what information posting online, once it is on the internet it is there forever.
- Secure Devices: Be sure to download applications only from trusted sources and keep operating system up-to-date, install anti-virus software and use a secure lock screen as well to prevent access of personal information.

  Protect identity: Be cautious when sharing personal ID such as name, address, phone number and/or financial information on the internet. Be sure websites are secure when making online purchases.
- Keep computer updated: By regularly updating computer, one can block attackers from being able to take advantage of software vulnerabilities. Security software essentials include firewall and antivirus programs. A firewall is usually computer’s first line of defense. Most internet browsers and Internet service providers provide a spam-blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails, from getting into inbox. However, every user must ensure to turn them on and do not turn them off. Also, users must install and keep up-to-date antivirus programs, firewalls and spyware checkers and make sure that they run the scans regularly.
- Call the right person for help: Try not to panic if become a victim. Just like any other crime report to local police. There are many websites to get help on cybercrime such as https://digitalpolice.gov.in, http://www.cybercrimehelpline.com
- Use Own Computer: - It's generally safer to access financial accounts from own computer only. If using some others computer, always delete all the "Temporary Internet Files", and clear all "History" after logging off account.
- Using Email: - A simple rule in using email is not to open any links in

emailsfrom stranger. Hackers do use E-mail as the main target seeking to stealpersonal information, financial data, security codes and other. Do not use the link sent. If need to access to any website, visit the website by typing the address in menu bar. Use secure website search, look for urls that starts with "https"

CONCLUSION

Cybercrimes will always be an ongoing challenge. Understanding the threat of cybercrimes is mandatory because technology holds a great impact on society as a whole. Cybercrime is growing every day since technological advancing and makes it very easy for anyone to steal without physically harming anyone. Cybercriminals are evolving in terms of computer knowledge per technological advancement made thus it is almost impossible to reduce cybercrime from the cyber-space. It is therefore recommend that every individuals and businesses need to make sure they are educated on what to do in terms of prevent in becoming the next victim of cybercrimes. This basic awareness can help prevent potential cybercrimes against them.

Conflict of Interest: None.

REFERENCES

1. Causes of Cybercrime and Preventive Measures. Available at https://krazytech.com/technical-papers/cyber-crime/amp. Accessed on 11/05/19
2. Available at https://shodhganga.inflibnet.ac.in/bitstream/10603/175612/9/09_chapter1.pdf. Accessed on 11/05/19
3. Available at https://www.government.nl/topics/cybercrime/forms-of-cybercrime. Accessed on 11/05/19
4. 11 ways to help protect yourself against cybercrime. Available at https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html. Accessed on 11/05/19
5. Cybercrime. Available at https://en.wikipedia.org/wiki/Cybercrime. Accessed on 11/05/19
6. Cybercrime Reporting Portal. Available at https://cybercrime.gov.in/cybercitizen/home.htm. Accessed on 11/05/19
7. Reporting Cybercrime. Available at https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/reporting-cybercrime/. Accessed on 11/05/19

How to cite this article: Begum F. Beware of cyber crime with awareness - a review. International Journal of Science & Healthcare Research. 2019; 4(3): 135-138.

******