Cyber Crimes and the Learner Pharmacist

Mr. Brajesh Kumar Choubey
Controller of Examinations, Asian International University, Manipur

Abstract— **Its time for the Learner Pharmacist to pause, look forward and understand the cobweb and the death like traps imposed on their daily use of the unavoidable computer in the modern world. They are to acquire that the web is not safe for all purposes. These days all the review of literature is on the computers through the innumerable websites of all tastes. The surfing and the use of websites should be dealt as if one is walking on thin ice! There are various types of crimes committed in the internet, making easy prey of the innocent users. So therefore the young learners in Pharmaceutical Education should be cautious and know about the "Cyber Crimes" or unlawful actions that are happening each second in the cyber world.**

BACKGROUND

The first recorded cyber crime happened within the year1820! That's not shocking considering the actual fact that the abacus, that is believed to be the earliest variety of a laptop, has been around since 3500 B.C. in India, Japan and china. The age of recent computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph – Marie jacquard, a textile manufacture in France, created the loom. This device allowed to repetition of a series of steps within the weaving of special materials. This resulted during a concern amongst jacquard's workers that their ancient employment and sustenance were being vulnerable. They committed acts of sabotage to discourage Jacquard from any use of the new technology. This is offer the primary recorded cyber crime! Nowadays computers have return an extended means, with neural networks and nano – computing promising to show each atom during a glass of water into a laptop capable of activity a billion operations per second. Cyber crime is associate n Nursing evil having its origin within the growing dependence on computers in trendy life. During a day and age once everything form microwave ovens and refrigerators to atomic power plants is being run on computer, cyber crime has assumed rather sinister implications. Major cyber crimes within the recent past embody the Citibank victimize. USA $10 million were fraudulently transferred out of the bank and into a checking account in Swiss confederation. The attack was perpetrated by a Russian hacker cluster junction rectifier by Vladimir Kevin, a notable hacker. The cluster compromised the bank's security systems. Vladimir was allegedly victimization his workplace laptop at AO Saturn, a computer firm in St. Petersburg, Russia, to interrupt into Citibank computers. He was finally inactive on Heathrow landing field on his thanks to Switzerland.

Defining cyber crime:
At the onset, let us satisfactorily define "cyber crime" and differentiate it from "conventional crime". Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. Defining cyber crimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation, sending threatening emails etc. A simple yet sturdy definition of cyber crime would be "unlawful acts wherein the computer is either a tool or a target or both".

Type of Cyber Crime
Most cybercrime falls under two main categories:

1. Criminal activity that targets computers.
2. Criminal activity that uses computers.

Cybercrime that targets computers often involves malware like viruses.
Cybercrime that uses computers to commit other crimes may involve using computers to spread malware, illegal information or illegal images.

List of Cybercrime examples:

1. Child Pornography or Child sexually abusive material
2. Cyber Bullying
3. Cyber stalking
4. Cyber Grooming
5. Online Job Fraud
6. Online sextortion
7. PUishing
8. Vishing
9. Smishing
10. Sexting
11. SIM Swap Scam
12. Credit Card Fraud or Debit Card Fraud
13. Impersonation and identity theft
14. Spamming
15. Ransomware
16. Viruses, Worms, and Trojans
17. Data Breach
18. Denial of Services (DoS) attack
19. Website Defacement
20. Cyber-Squatting
21. Pharming
22. Cryptojacking
23. Online Drug Trafficking
24. Espionage, etc.

Let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Some examples are:

Financial crimes:
This would include cheating, credit card frauds and money laundering. Here people may use a false or bogus website, providing their credit card numbers to buy a certain product. The bogus website then flee, taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.

Cyber pornography:
This would include pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). One Indian incidents revolving around cyber pornography include the Air Force Balbharati School case. A student of the Air Force Balbharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.

Sale of illegal articles:
This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

Online gambling:
Many websites today offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

Intellectual Property crimes:
These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

Email spoofing:
A spoofed email is one that appears to originate from one source but actually has been sent from another source. Here, the learner Pharmacist should be careful, as many e-mail can come in, tantalizing with lottery winning and gift offering.

Forgery:
Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high quality scanners and printers. In fact, this has become a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.

Cyber Defamation:
This occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone

publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

Cyber stalking:
The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.
Now let us examine some of the acts wherein the computer is the target for an unlawful act. It may be noted that in these activities the computer may also be a tool. This kind of activity usually involves sophisticated crimes usually out of the purview of conventional criminal law.

Password cracking
A password is a type of authentication. It is a secret word or phrase that a user must know in order to gain access. A pass-phrase is a correspondingly larger secret consisting of multiple words. Use of Passwords dates back to the Roman times. The Romans were some of the first large armies where people didn't recognize each other by sight. In order to gain entry into the camp, a Roman soldier would have to know the secret password.
Internal to the computer, password information is constantly being checked. If you were queried for the password each and every time, you would find that computer would become unusable. Therefore, the computer attempts to "cache" the password so that internal prompts during the same session do not cause external prompts to the user.
All systems cache passwords in memory during a login session. Therefore, if a hacker can gain access to all memory on the system, he/she can likely shift the memory for passwords. Likewise, hackers can frequently shift page files for passwords. To crack a password means to decrypt a password, or to bypass a protection scheme.
Learner Pharmacist should be aware of these facts, and see to their protection of passwords and safely “LOG OUT” of the system , never share their pass words with others.

Theft of information contained in electronic form:
This includes thefts of information stored in computer hard disks, removable storage media etc & Theft of computer system: This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

Physically damaging a computer system:
This crime is committed by physically damaging a computer or its peripherals.

Data diddling:
This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems. Research data is normally being stored by learner Pharmacist, and this knowledge will help them to treasure them carefully.

E-mail bombing:
This involves crashing of servers or overloading of networks by sending huge amounts of junk e-mail. Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. In one case, a foreigner who had been residing in Shimla, India for almost thirty years wanted to avail a scheme introduced by the Shimla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Shimla Housing Board and repeatedly kept sending e-mails till their servers crashed.

Internet time thefts:
Learner Pharmacists may note seriously that this connotes the usage by an unauthorized person of the Internet hours paid for by another person. This usually happens when the ID and password for access to the internet of the user is stolen by another , and start using it unauthorized manner. The huge bill that comes in later to the owner opens the eyes.

What has the Indian law to say?

Section 441 of the Indian penal code says that “whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property ,unlawfully remains there with intent thereby to intimidate ,insult or annoy any such person, or with intent to commit an offence ,is said to commit criminal trespass.

Section 425 of the code says that: “whoever with intent to cause ,or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property ,or any such change in any property or in the situation thereof as destroys or diminishes its value or utility or affects it injuriously ,commits mischief”

Whether information sourced in a computer can be defined as property should be resolved unambiguously.

Penalties, offences and authorities under the Information Technology Act 2000

Penalties under the Act

Section 43 of the Information Technology Act lists the various acts for which a person will be liable to pay damages by way of compensation up to Rs. 1 crore.

Offences under the Act

Sections 65 through 74 of the Information Technology Act, 2000 (the Act) contain provisions relating to various cyber crimes. The maximum imprisonment provided for by the IT Act extends to 10 years.

CONCLUSION

The use of computer today by each person has become inevitable. Anyone without computer knowledge is termed as “illiterate”. As the literacy rates are soaring heights, more and more computer use is taking place. Pharmacist learners are no exception. They stride along with other streams of discipline. The use of computers for reference and review of literature are being depended upon. Besides surfing for other information, chats and being on face book and twitter for being with friends and social circle. The use of computer has become easier for large storage of data at one place (unlike the use of paper files during earlier days), and becoming very convenient for access to data while sitting anywhere in the Globe.

Computer users, especially those who frequently visit websites and use them for either knowledge or fun can simply remember the tips given here and safeguard themselves.

REFERENCE

[1] https://123dok.com/document/z3exdleq-introduction-to-cyber-crime.html"\l":~:text=Defining%20Cyber%20Crime,to%20the%20Indian%20Penal%20Code.

[2] www.sanglipolice.gov.in/contentpage/cyber_crime

[3] https://www.trademarkiso.com/law/cyber-crime-it-act/

[4] https://www.ijser.org/researchpaper/CYBER-LAW-AND-INFORMATION-TECHNOLOGY.pdf

[5] https://www.legalservicesindia.com/articles/cyber.htm/

[6] https://www.researchgate.net/publication/338441815_UNDERSTANDING_CYBER_CRIME_AND_CYBER_LAUNDERING_THREAT_AND_SOLUTION/

[7] https://www.recoveryandforensic.com/cyber-crime-investigation/

[8] "https://www.greaterkashmir.com/gk-magazine/crime-of-the-modern-age

[9] https://nagpurgraminpolice.gov.in/eng/index.php?link=branches&branch_id=Mg==&lan=eng/

[10] https://www.coursehero.com/file/80971371/Introduction-to-Cyber-Crimepdf/

[11] https://indiaforensic.com/classification-of-online-frauds/

[12] https://www.bing.com/ck/a?!" \t

[13] http://www.cyberlawclinic.org/cybercrime.htm"\l ":~:text=E%2DMail%20spoofing%3A,termed%20as%20E%2DMail%20forging.

[14] https://indiaforensic.com/classification-of-online-frauds

[15] https://blog.ccasociety.com/cyber-crime-definition-types-and-prevention

[16] https://www.karnikaseth.com/what-is-cyber-defamation.html

[17] https://writers-corp.net/admin/get_sample/cyber-laws-and-cyber-crime

[18] https://redteamacademy.com/cyber-violence-against-women

[19] http://www.penacclaims.com/wp-content /uploads/2020/12/Yashwanth-AS.pdf/

[20] https://indiaforensic.com/certifications/classification-of-online-frauds/" \t

[21] https://lawcyber.blogspot.com

[22] "https://books.google.com/books?id=M7PIVPmYoXoC"

[23] http://web.tiscali.it/carlogabbi/pc%20dictionary.html" \t