CYBER SECURTIY: ESTIMATION OF CYBER SECURITY AWARENESS QUOTIENT OF YOUTH

BY -

AJINKYA DANDGAVHAL

INDEX

INTRODUCTION

In this age of technology, the use of computers is increasingly spreading and more and more users are getting connected to the internet. The rapid growth and development of technology has also given rise to a completely different and technologically advanced form of crime called the cyber crime. Cyber Crime includes hacking, copyright infringement, gaining unlawful access to someone's bank account or email account using illegal means, child pornography, financial theft, phishing etc. These crimes have virtually no boundaries and may affect any country across the globe within a fraction of seconds. Following are some statistics regarding internet users in India.

Internet Users in India (2016): 462,124,989 (46.2 Crore)

Share of India Population: 34.8 % (penetration)

Total Population: 1,326,801,576

Share of World Internet Users: 13.5 %

Internet Users in the World: 3,424,971,237 (342.4 Crore)

In simple words Cyber Crime can be defined as "any crime that takes place over the Internet". In broader sense Cyber Crime can be defined as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victims or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as internet and mobile phones". To prevent becoming a victim of cyber crime, we need to know about cyber security.

Cyber Security, also known as IT security, is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide. Cyber security includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection.

The field is of growing importance due to increasing reliance on computer systems and the internet, wireless networks such as Bluetooth and Wi-Fi, including smartphones etc.

There are two major types of risks while surfing online. One is the technological risk, which comes as a result of dangerous software and "Bugs" in the programs we use. Second is the behavioural risk which relates to the decisions we make online. This includes not thinking before clicking on links or opening emails or downloading any attachment sent by an unknown person.

Cyber security often depends on decisions made by human operators, who are commonly considered a major cause of security failures.

These risks can be minimized if we take simple precautions while surfing online like setting a strong password for online accounts, not sharing your passwords with anyone, using regularly updated version of antivirus software etc.

The majority users on the internet are the young boys and girls who fall in the age group of 18-30 years. Mostly this is the age when people are most energetic and full of enthusiasm and also highly impatient. They cannot wait to share photos, messages, download newly released movies or songs etc. They usually don't think before clicking. This makes them highly vulnerable to cyber crime. Sharing personal information, data or even photos and messages can lead them to becoming the victims of cyber crime. Not being cautious enough while being online is an open invitation for hackers and online fraudsters to hack into your account and steal your valuable information that sometimes might cause you to lose money.

Simple behavioural changes like being cautious of unknown emails, not downloading attachments that are mailed to you by some unknown person, setting strong passwords and not sharing your passwords with anyone can help you stay immune to cyber threat.

Through our project "Cyber Security" we aim to estimate the Cyber Security Awareness Quotient of the students between age group of 18-30 years. i.e. we simply wish to test how aware today’s youth is about cyber crime and the precautions they need to take to prevent being the victims of it.

This we will do by designing a small quiz (MCQ type) that contains some basic questions and situations where the person has to mark his response or reaction which he will take if faced with such a problem in real life. Also the quiz will test their basic cyber awareness. We will compute the scores of each student that is based on how many questions he answers correctly and will then decide how well aware he is regarding cyber security.

Also, we have analyzed and interpreted secondary data regarding cyber crime in India using bar-graphs, pie-charts, and tables. We have calculated % variation regarding the no. of crimes and arrests made during year 2014-15. Further we have tried to find pattern in the no. of cases registered for cyber crime. Also, using pie-chart we have found out the age group wise distribution of the arrests made regarding cyber crime and the age group that commits maximum amount of crime.

In the end we have suggested some simple but important tips to keep one safe from cyber attacks. If these tips are kept in mind and practiced while surfing online, we feel that it will reduce the risk of cyber threat by a large amount.

We aim to achieve the following objectives through our project:

1. Analyse secondary data on cyber crime and interpret and represent it using various tools and diagrams.
2. To estimate how aware today's youth is regarding cyber security using cyber security awareness quiz.
3. To check whether gender is related to the cyber security awareness level using chi-sq test.
4. To check whether basic awareness about cyber security is effective in improving the awareness level using paired-t test.
5. Suggest tips for safe surfing and ways in which one can prevent becoming a victim of cyber crime.

RESEARCH METHODOLOGY

This project aim to estimate the Cyber Security Awareness Quotient of the students between age group of 18-30 years i.e. we wish to test how aware today's youth are about cyber crime and the precautions they need to take to prevent being the victims of it.

This has been done by designing a small quiz (MCQ type) that contains some basic questions and situations where the person has to mark his response or action which he will take if faced with such a problem in real life. Also the quiz will test their basic cyber awareness. We then computed the scores of each student that is based on how many questions he answered correctly and have then decided how well aware he is regarding cyber security. This quiz was distributed among a sample of 250 students.

Also, we wish to test, is gender and cyber security awareness quotient independent or dependent. We have done this by using Chi-Square test of independence of attributes.

Further we took a sample of 10 students from these 250 students. We provided them with basic awareness about cyber security i.e. how to set strong passwords, how to recognize if a mail is fraudulent, what is botnet, ransomware, malware, how to check if a site is fake etc. Then we once again asked them to fill the quiz and recorded their scores. Using this data we wish to test the effectiveness of the basic awareness which we have provided to the students by testing whether their scores showed improvement or not. This we have done using paired t-test.

LAWS IN INDIA TO CONTROL CYBER CRIME

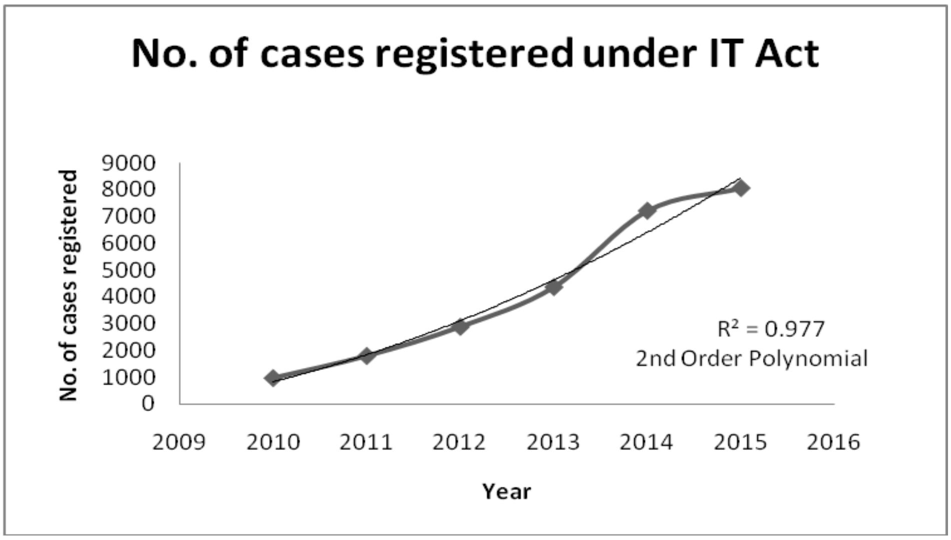
There are two laws in India regarding cyber crime. One is the Indian Penal Code Section and the second one is the Information Technology Act, 2000. They are as follows:

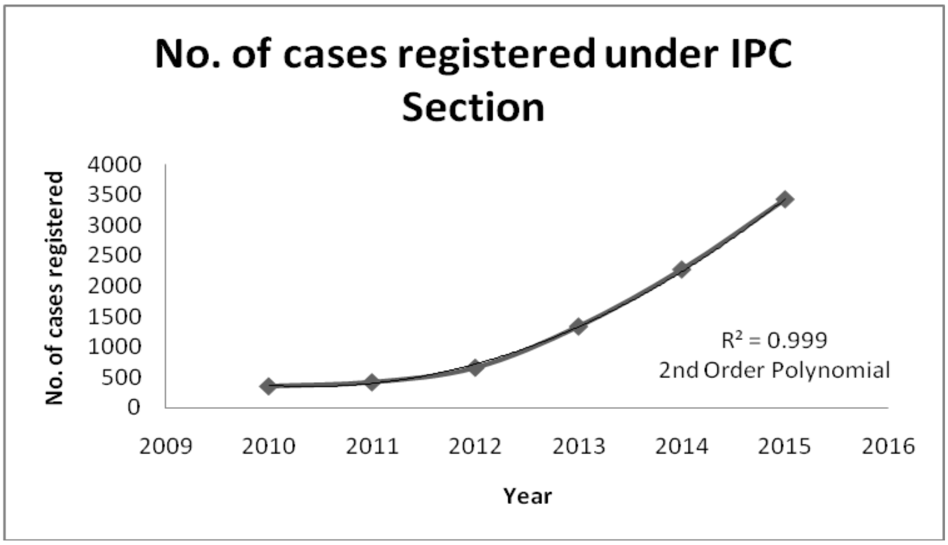
Offences under the Information Technology Act, 2000	Offences under the Indian Penal Code, 1860
Tampering with computer source documents	Offences by/against public servant
Hacking with computer systems	False electronic evidence
Obscene publication/ transmission in electronic form	Destruction of electronic evidence
Unauthorised access/ attempt to access protected computer system	Forgery
Breach of confidentiality/privacy	Criminal breach of trust/fraud
Obtaining licence of digital signature certificate by misinterpretation/suppression of facts	Counterfeiting currency/ stamps, mark etc
Publishing false digital signature certificate	
Other	

DATA ANALYSIS

Incidence of cases registered under cyber crimes in India under IT Act, 2000 and IPC Section.

Year	IT Act	IPC Section	Total
2010	966	356	1322
2011	1791	422	2213
2012	2876	661	3537
2013	4356	1337	5693
2014	7201	2272	9473
2015	8045	3422	11467





It can be seen from the above table that no. of cyber crimes are increasing rapidly with 1322 crimes in 2010 and 11647 crimes in 2015 i.e. an overwhelming 781% increase in the total no. of crimes. Also, in both the graphs i.e. the no. of crimes registered under IT act and IPC section, both follow 2nd order polynomial trend with a steep increase in the no. of crimes between year 2013 and 2014.

CYBER SECURITY AWARENESS QUESTIONNAIRE

Gender □ Age □

1. Who is it OK to share passwords with?

□ Your Boss

□ Your Co-worker

□ Human Resources

□ Close friends or family

□ None of the above

2. True or False. If you use a public Wi-Fi network (in a café or hotel, for example) that assigns you a password, it's okay to send confidential business data or do online transactions.

□ True

□ False

3. What tips should you follow when opening attachments or links? (Check all that apply)

□ Make sure your antivirus is up to date

□ If a message comes from someone you know personally, it's okay to open or click them.

□ Don't open or click links if they appear out of context- for example, ilovegreenpines.pdf from your boss.

□ Look carefully at the link or attachment if it's safe to open.

□ View everyone with suspicion

4. How can you tell if an email is fraudulent? (Check all that apply)

□ Unfamiliar email address

☐ Alarmist messages urging you to take action as soon as possible

☐ Grammatical errors

☐ Account related requests, such as asking for login information or passwords

5. What does the “https://” at the beginning of a URL denote, as opposed to "http://" (without the “s”)?

☐ The information entered into the site cannot be copied

☐ The information entered into the site is locked

☐ The information entered into the site is encrypted

☐ The information entered into the site cannot be viewed

6. Which of the following is an example of a “phishing” attack?

☐ A mail from bank asking you to send them your account information.

☐ A mail saying that you have won a certain luck draw and to claim the prize send them your personal information like mobile number, address, account information etc.

☐ Call from a clerk from your bank asking you to provide your debit card information to renew your card’s validity as it is going to expire soon.

☐ All of the above

7. A group of computers that is networked together and used by hackers to steal information is called a .....

☐ Rootkit

☐ Botnet

☐ DDoS

☐ Darknet

8. Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication?

□ 7862 (otp)

□ ~~ULqo0~~ (captcha)

□ Security Question

□ Not Sure

9. Which among following four passwords is the most secure?

□ 942656989

□ Greenapple

□ Wh@t5!tZ

□ Mike123

10. Criminals access someone’s computer and encrypt the user’s personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called …

□ Malware

□ Ransomware

□ Driving

□ Phishing

11. “Private browsing” is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?

□ Yes

□ No

12. Turning off the GPS function of your smartphone prevents any tracking of your phone’s location.

- □ True
- □ False

This is the Cyber Security Awareness Quiz. This quiz was distributed among 250 students in the age group of 18-30 years. The scores were evaluated and the following conclusions were obtained after analyzing the data.

DATA INTERPRETATION

1. Who is it OK to share passwords with?

   The correct answer is “None of the above”. Passwords should never be shared with anyone, not even close friends and family members. Passwords protect your valuable data, so, always keep it secret.
   Correctly: 71%

2. True or False. If you use a public Wi-Fi network (in a café or hotel, for example) that assigns you a password, it’s okay to send confidential business data or do online transactions.

   The correct answer is “False’. Even if a public Wi-Fi network requires a password, other users can potentially view the sensitive information a user sends across that Wi-Fi network.
   Correctly: 74%

3. What tips should you follow when opening attachments or links? (Check all that apply)
   All the options are right except the second one. Even if a mail is from someone you know personally, you should still be cautious while opening the mail. There are some viruses which send their own copies as attachments to the first few contacts in the mail address list from the account which they have infected.
   Correctly: 3%

4. How can you tell if an email is fraudulent? (Check all that apply)
   All the options are correct.
   Correctly: 2%

5. What does the “https://” at the beginning of a URL denote, as opposed to "http://" (without the “s”)?

The correct answer is “The information entered into the site is encrypted”. Encrypting information entered into a website makes it far more difficult for anyone other than the user and website owner to read the information. As of February 2017, around half of all internet traffic is now encrypted.

Correctly: 43%

6. Which of the following is an example of a “phishing” attack?

All the options are examples of phishing attack. Phishing attacks attempt to get a user to click on a malicious link or file by impersonating a trusted source the user is familiar with.

Correctly: 46%

7. A group of computers that is networked together and used by hackers to steal information is called a …..

The right answer is “Botnet”. A rootkit is a type of malicious software designed to gain unauthorized access to a computer system. DDoS stands for Distributed Denial of Service, it is an attack where large amounts of requests are sent to a web server in order to overwhelm the server and shut it down.

Correctly: 27%

8. Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication?

The correct answer is “7862 (otp)”. This is the only example of two-step authentication listed – true two-step authentication requires the user to enter a one-time code each time they log in to their account, in addition to their regular username and password. While the other answers may require users to perform two separate operations to gain access to a site, they are not examples of two-step authentication.

Correctly: 7%

9. Which among following four passwords is the most secure?

The correct answer is “Wh@t5!tZ”. This password is strong as it is a combination of upper case, lower case letters, digits and special symbols.
Correctly: 82%

10. Criminals access someone’s computer and encrypt the user’s personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called …

The right answer is “Ransomware”.

Correctly: 5%

11. “Private browsing” is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?

The right answer is “Yes”. Private browsing prevents a user’s internet browser from storing certain kinds of files on his or her device. However, internet service providers can still see all of the details of the user's web traffic.

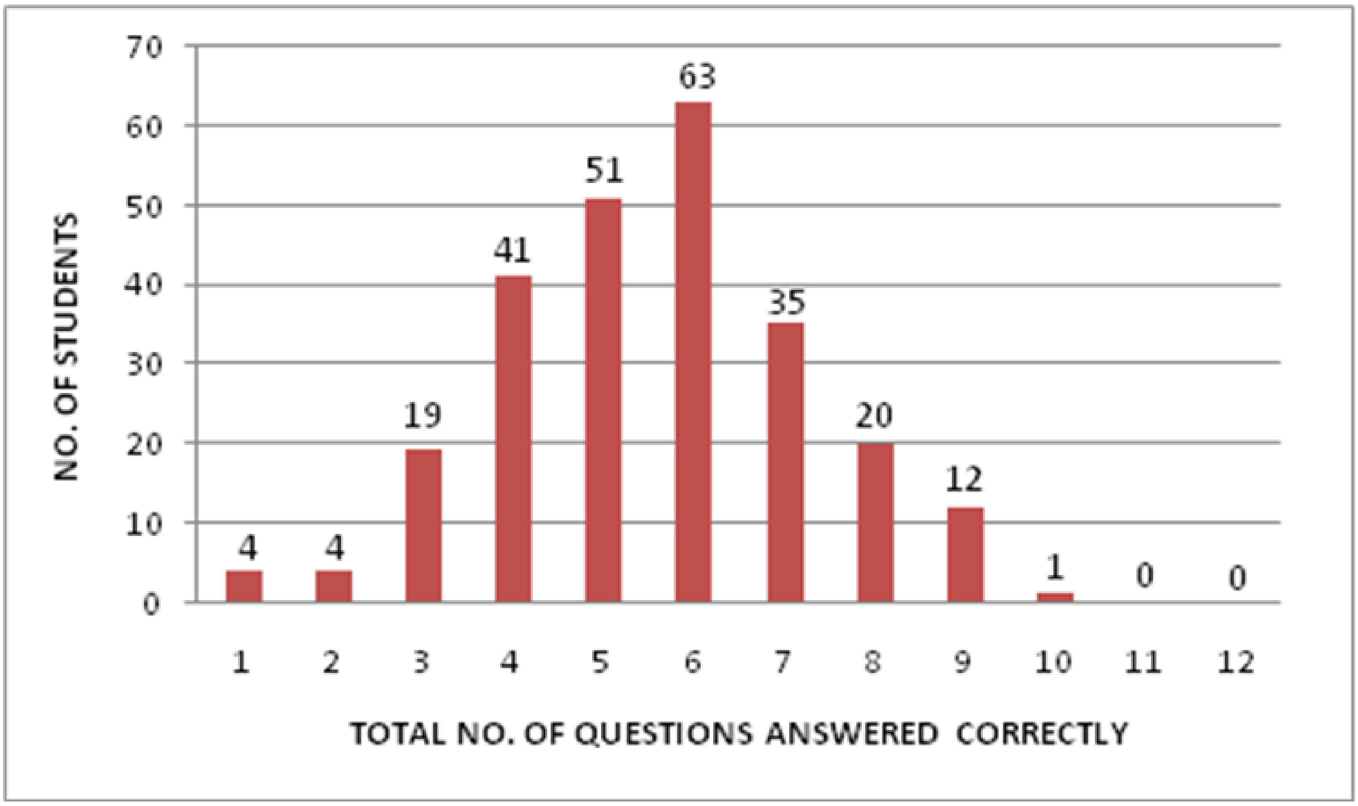
Correctly: 52%

12. Turning off the GPS function of your smartphone prevents any tracking of your phone’s location.

The correct answer is “False”. In addition to GPS, smartphones can also be tracked using the cellphone towers or Wi-Fi networks that the phone is connected to.
Correctly: 40%

WHAT THE YOUTH KNOWS ABOUT CYBER SECURITY

A majority of youth can answer fewer than half the questions correctly on a knowledge quiz about cyber security issues and concepts.



1. A majority of online youth can identify a strong password (82%) when they see one and recognize the dangers of using public Wi-Fi (74%). However, many struggle with more technical cyber security concepts, such as what is a phishing attack or determine if a webpage they are using is encrypted.

2. This quiz consisted of 12 questions designed to test the youth's knowledge of a number of cyber security issues and terms. Cyber security is a complicated and diverse subject, but these questions cover many of the general concepts and basic building blocks that cyber security experts stress are important for users to protect themselves online. However, the typical (median) respondent answered only 6 of these 12 knowledge questions correctly (with a mean of 5.556 correct answers). One-in-eight (13.2%)

answered more than eight questions accurately, and just 1 in 250 received a score of 10. No one was able to answer all the questions correctly. These are the key findings from the survey of 250 youths.

3. Cyber security knowledge varies widely by topic and level of technical detail.

4. Of the 12 questions in the quiz, a substantial majority of youth was able to correctly answer 6 of them. First, 82% of young internet users can correctly identify the strongest password from a list of four options.

5. Many (72%) are aware that if a public Wi-Fi network is password protected, it does not necessarily mean that it is safe to perform sensitive tasks, such as online banking, using that network.

6. Meanwhile, around half of internet users are able to correctly answer several other questions in the survey. Some 46% of young internet users are able to identify examples of phishing attacks. A similar share (48%) can correctly define the term "ransomware." This refers to criminals accessing someone's computer, encrypting their personal files and data, and holding that data hostage unless they are paid to decrypt the files.

7. Also, 40% correctly say that turning off the GPS function of a smartphone does not prevent all tracking of that device (mobile phones can also be tracked via the cellular towers or Wi-Fi networks to which they are connected).

8. The youth's understanding of some practical issues is very poor. Very small percentages (2.8%) of young users are aware about the precautions they should take while opening email attachments or links. Also, only 1.6% of the users know what a fraudulent email looks like. Public knowledge of cyber security is lower on some relatively technical issues like botnet (27%), two-step authentication (7.2%).

9. Internet users' understanding of the remaining cyber security issues measured in the survey is lower. For instance, 54% of internet users are aware that internet service providers (ISPs) are able to see the sites their customers are visiting while utilizing the "private browsing" mode on their internet browsers. Private browsing mode only

prevents the browser itself, and in some cases the user’s computer or smartphone, from saving this information – it is still visible to the ISP. And 43% are aware that the letter “s” in a URL beginning with “https://” indicates that the traffic on that site is encrypted.

10. Meanwhile, just 27% of young users are aware that a group of computers that is networked together and used by hackers to steal data is referred to as a “botnet”.

11. Lastly, cyber security experts commonly recommend that internet users employ “two-factor” or “multi-factor” authentication on any account where it is available. Two-factor authentication generally requires users to log in to a site using something the user knows (such as a traditional password) along with something the user possesses (such as a mobile phone or security token), thus providing an additional layer of security in the event that someone’s password is hacked or stolen. Just 7% of users are able to correctly identify the example in the list of a true multi-factor authentication process. In this case, the correct answer was a picture of a temporary code sent to a user’s phone that will only help them login for a limited period of time. Several of the other answer options illustrated situations in which users were required to perform a secondary action before accessing a page – such as entering a captcha, or answering a security question. However, none of these other options are examples of two-factor authentication.

12. Also, 70% are aware that passwords should not be shared with anyone.

CHI-SQUARE TEST

Here, we have performed chi-square test to test whether gender and cyber security awareness level is related or not. Following table is a 3X2 contingency table. The findings are as follows:

Awareness/ Gender	Male	Female	Total
Poor (1-4)	34	34	68
Moderate (5-8)	88	81	169
Good (9-12)	3	10	13
Total	125	125	250

We have used chi-square test for independence of attributes.

Hypothesis is:

Ho: Attributes are independent

H1: Attributes are dependent

Test Statistic:

χ^2_{calc} = 4.059171

Table Value:

$\chi^2_{2critical}$ = 5.991 (at 5% l.o.s)

As,

χ^2_{calc} = 4.059171 < $\chi^2_{2\ critical}$ = 5.991 (at 5% l.o.s)

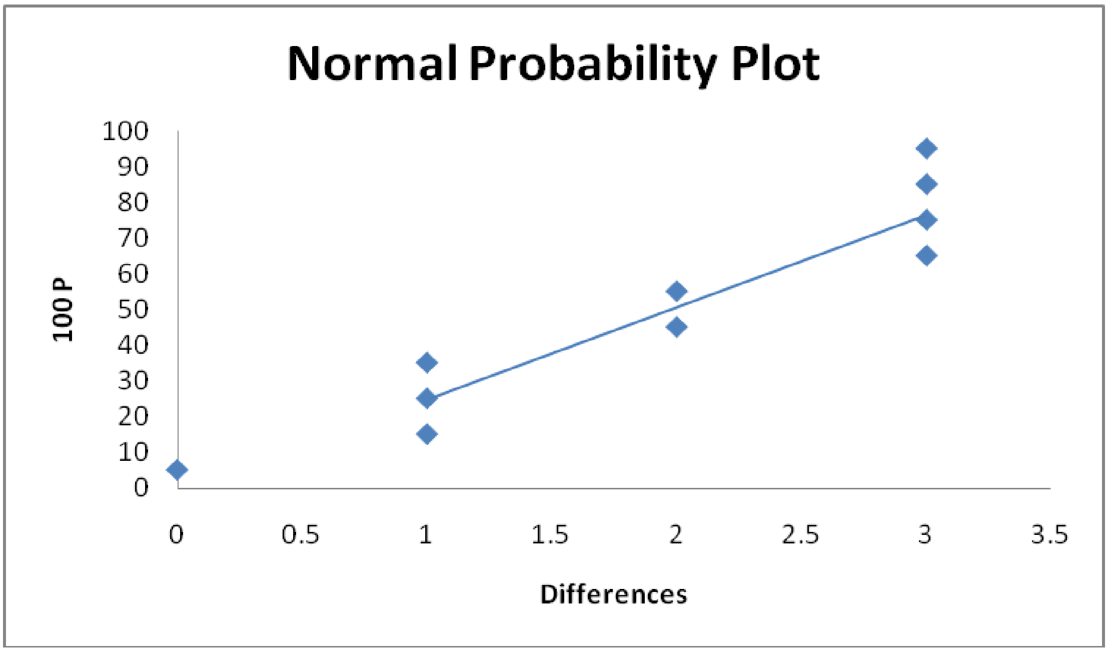
We accept Ho

Therefore, we accept Ho. i.e. attributes are independent. That means gender and cyber security awareness level is not related.

PAIRED-t TEST

Here, we have performed paired-t test to test whether the basic awareness which we provided to a sample of 10 students was effective in improving their cyber security awareness or not. Following are the findings:

Before	3	8	3	6	7	1	6	3	7	4
After	5	8	6	9	8	4	9	2	8	6



From the above Normal Probability Plot we can see that the differences are normally distributed. So, we can use Paired-t test.

Hypothesis is:

Ho: $\mu_d = 0$

H1: $\mu_d > 0$

Test Statistic:

$\mathbf{t}_{\mathbf{calc}}$ = 3.34

Table Value:

$\mathbf{t}_{\mathbf{critical}}$ = 2.262 (at 5% l.o.s)

$\mathbf{t}_{\mathbf{critical}}$ = 3.250 (at 1% l.o.s)

As,

$\mathbf{t}_{\mathbf{calc}}$ = 3.34 > $\mathbf{t}_{\mathbf{critical}}$ = 2.262 (at 5% l.o.s)

$\mathbf{t}_{\mathbf{calc}}$ = 3.34 > $\mathbf{t}_{\mathbf{critical}}$ = 3.250 (at 1% l.o.s)

We reject Ho

Therefore, we reject Ho; accept H1 .i.e. $\mu_d > 0$. It implies that the basic awareness which we provided to a sample of 10 students was effective in improving their cyber security awareness.

From the above test we can infer that to improve the level of awareness and prevent young internet users from becoming victims of cyber crime we can organize simple awareness campaigns, or include some basic tips for safe surfing in the academic curriculum or just provide them with the basic awareness in the form of emails, posters, whatsapp messages, lectures etc.

CONCLUSION

In an increasingly digital world, an individual’s personal data can be as valuable and as vulnerable to potential wrongdoers as any other possession. Despite the risk-reducing impact of good cyber security habits and the prevalence of cyber attacks on institutions and individuals alike, our survey finds that many young internet users are unclear about some key cyber security topics, terms and concepts. A majority of the youth are between poor to moderately aware regarding cyber security.

From the above tests we can infer that to improve the level of awareness and prevent young internet users from becoming victims of cyber crime we can organize simple awareness campaigns, or include some basic tips for safe surfing in the academic curriculum or just provide them with the basic awareness in the form of emails, posters, whatsapp messages, lectures etc.

Also, it comes out that gender and cyber security awareness level are not related. So, everyone is at an equal amount of cyber risk. So, one must better equip oneself with the necessary knowledge of cyber security and put it to practice in everyday life.

Some simple precautions practiced when surfing online can save you from lots of trouble. On the next page is a list of tips which we think that every individual must know to guard him/her from the pirates of the cyber world. Make sure you know them well and practice them in everyday life.

TIPS FOR SAFE SURFING

1. Make strong passwords: A strong password should not be smaller than eight letters. Make use of uppercase letters, lowercase letters, a few numbers and some special symbols. Ex. Banana can be made into a strong password by changing some of the letters in it. Example B@n4N@
2. Clear your cache, erase history, and log out: It's important to log out to prevent others from accessing your account. History or cookies can be used to gain information about user preferences, credit card information, login information, activity history etc. So, always remember to clear history and cookies.
3. Keep your software up to date: Software makers often release patches, fixes and updates to address newly discovered bugs and security threats. By routinely updating your software you can prevent these threats.
4. Use antivirus/anti-malware software: Invest in this powerful line of defense, learn to set it up, keep it updated, and let it do its job. Some well known brands of software are Quick Heal, Avast, Norton.
5. Secure your router and wireless network: Set a strong password for your wireless router so that nobody outside of your household can access it.
6. Know how to recognize a secure site: A secure site encrypts the data that is transmitted between it and your computer. This means that for the duration of transmission the information is secure. Secure sites are indicated by a web address that starts with "https" (instead of just "http") and a padlock icon at the top or bottom right of your browser window (not the website itself).
7. Use privacy tools: Social media sites and browsers offer tools that allow you to customize the amount of personal information you share with other users. Take the time to read, understand and use these settings. Another privacy tool provided by browsers - private browsing – lets you surf the web without leaving personally identifying records in cache files on the computer of where you've been. (It's important to keep in mind, though, that private browsing only applies to the computer you are using. Your internet service provider or other application may still save records).

8. Be careful of emails: Be careful of emails from unknown email addresses. Never click a link that looks out of context even if it's from the person you know. Often it's a virus.
9. Be careful while uploading anything on social media: Always be careful while uploading, sharing, forwarding any media or message on social media websites. Think twice about what you are uploading; ask yourself whether it is relevant and not offensive.
10. Turn off the GPS: GPS can be used to track tour location. So, switch it off when not required. Also, turning off the GPS does not guarantee that you'll not be tracked. Your location can be tracked using cell phone towers and also if you're connected to some public Wi-Fi, even then you can be tracked.
11. Beware of Public Wi-Fi: Never make any online transaction using a public Wi-Fi (like at airports or hotels) even if it assigns a password to you. These can be hacked easily and your account security might be compromised.
12. Beware of fake calls and emails: Any call or email from a bank clerk asking for your account or login details is 101% fake. No bank calls a customer for such details. So, always be careful of such calls.

BIBLIOGRAPHY

1. www.pewinternet.org
2. www.mediasmarts.ca
3. www.wikipedia.org
4. www.microsoftbusinesshub.com
5. www.cybersecuritymonth.eu
6. Cyber Security tip sheet of Canadian Internet Registry Authority (CIRA)
7. National Crime Records Bureau’s (NCRB) Annual Crime Report.
8. Cyber Crimes in India 2012-13: Facts and Measures by Dr. B.D. Karhad