International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Awareness of people about identity theft & Cyber-crime while using internet

Kalpak Vijay Rasam

ASM's Institute of Management & Computer Studies

Cyber-crime is one of the biggest drawbacks of technological development in the world where internet is turning into one of the basic prerequisites in almost all fields and branches of studies.

The present study covers details about cybercrime also in what kind they take place, ruining lives of lakhs of people across the globe on daily basis. Stealing identity of an individual, known as individua theft, poses great threat to the mankind.

Such practices are one of the few examples of missing technology. The survey was conducted during experimentation. An analysis is done to explore the awareness of cybercrime among common people, who are major target of such criminal-minded maniacs.

As internet is gradually turning into one of the basic obligations for people belonging to different walks of life, cyber-crime acts as a major challenge in the expansion and development of widespread use of the internet.

Cyber-crimes take place using a computer which is considered as an "object or subject of the conduct constituting crime." Computers are accessible and store whole lot of different kinds of data and in a small space, which tend to make them assailable to such criminals. Cyber criminals target children, youth or teenagers, adolescents, professional hackers and acrimonious employees. The term 'cyber' can be anything relating to or some kind of characteristics of the civilization of computers, information technology, and virtual reality. For this purpose, a computer may have been used to act such a heinous crime or simply a computer may be the target. These crimes include and are not always limited to identity theft, foreboding a nation's safekeeping, copyright infringement and child pornography. These crimes have become a colossal threat to individual privacy, where confidential data individual's identity or photos and videos are stolen or ambushed by the attacker. In Cyber Crime, such as identity theft, financial theft, espionage, most of the times non-state agents and also government organizations are involved. Cybercriminals usually use computer technology to ingress and accrued personal information, business trade secrets or use the internet to attain coercive or malicious objectives. Criminals can also use computers for communication, hacking or accessing data storages apparently. Criminals who carry out these illegal activities are often to as hackers. Because of the peculiar nature of cyber-crimes, they can be committed mysteriously and far away from the victim without existing physically. Also, cyber criminals are kind of vulnerable creatures that can use computer technology to cause damage to anyone without the fear of being caught.

Types of Cyber Crimes:

Cybercrimes can be addressed as crimes that occur by the means of computers or other devices such as hacking. In cyber-crimes, computers or other devices are used fundamentally to conduct a wide range of breaches such as online fraud, identity theft and the distribution of child exploitation material. The drastic effects of cybercrime can be extremely upsetting for victims, and it isn't always necessarily just for financial reasons. There might be other reasons too. Victims of such crimes are so terrified that they develop an

unthrusting mindset feeling that their privacy has been seized, and that they are powerless Overall, most common types of cyber-crimes that are seen frequently occurring across countries, cyber-attacks and various other internet ambiguous activities are: attacks on computer system, cyber-bullying, prohibited offensive and illegal content, online child sexual abuse material, spam email and phishing emails. Some other activities like digital piracy, money laundering, and counterfeiting are seen in many cases related to cyber- crime across the globe. The major cyber-crimes are categorized into different categories

Attacks on Computer System: Cyber-criminals are not only crafty minded people, but they are also citified and are able to exploit susceptibilities on computers and other devices. Some of the techniques used by such criminals on the web also comprise unauthorized access or hacking, malware and denial of service attacks. Attacks can result in a criminal accessing personal or financial data of an individual, preventing them from being able to use their devices or computer system consequently.

Cyber-bullying: Cyber-bullying also knows as web stalking. This is a situation where in a intruder who engages in offensive, alarming or harassing behaviour through the internet or technology. It can happen to individuals belonging to any age-group, and at any time, irrespective of the motives for behind such a crime committed and often anonymously. Examples of cyber-bullying include

- Posting hurtful messages, images or videos online
- Repeatedly sending unwanted messages online
- . Sending abusive texts and emails
- Excluding or intimidating others online
- Creating fake social networking profiles or websites that are hurtful
- . Nasty online gossip and chat
- Form of digital communication, which is discriminatory, intimidating, intended to cause hurt or make someone fear for their safety

Email Spam and Phishing: Spam is electronic junk mail- unsolicited messages sent by email, text message or an instant message without the recipient's permission. Phishing is a means by which cyber-criminals trick people in a way that they give out their personal or financial details. Phishing messages often pretend to come from genuine-looking businesses, such as banks or telecommunications providers, on whom ordinary people fall prey very easily.

Identity Theft: Identity theft happens when a criminal gains access to the personal information such as name, address, date of birth or bank account details to ransack money or to gain other benefits. Criminals may attempt to gain personal information using several different techniques, including

- ‘Phishing’-one may provide personal information over the phone or internet to what appears to be a real-life business, but is a huge scam,

- Hacking one's online accounts,
- Obtaining personal information from social media, and
- Illegally accessing information about which is stored on a business database.

Online child sexual abuse material: Any material that displays or illustrates child sexual abuse and other related offences against children are illegal. It is an offence to access, possess, distribute, produce, advertise or make available child pornography or any other child abuse material either online or using any other mediums of transmission. Procuring, grooming or engaging a person less than 16 year of age in sexual activity, or sending indecent messages and comments to a juvenile. Cybercrime has major effects on both a virtual and a real body, but the effects upon each are completely different. This phenomenon is seen very clearly in the case of identity theft.

Identity theft and its consequences: Identity theft, sometimes referred to as identity fraud, is a crime in which a pretender procures key pieces of personally identifiable information, such as social security or driver's license numbers, in order to impersonate the targeted individual, The more the fraudsters discover different and more complex approaches to gather the information which is required to steal an individual's identity. Identity theft occasionally involves the unlawful ways to take a victim's personal details. However, it does involve the perpetrator of the crime who obtains the victim's personal information and then uses this in an illegitimate way for their own personal gains. The identity theft happens in following ways.

Lost or Stolen Personal Documents: Although most of the consumers are seen storing and depositing a lot of information online, studies have indicated that how this has led to an increase in identity theft cases. A typical person's wallet comprises an abundance of a lot of sensitive personal details, such as credit cards, driver's license, and sometimes even contact numbers, which identity thieves can use to carry out purchases, open new lines of credit, do housing, and also apply for loans. A wallet is just one of the typical examples that describe how and what kind of physical resources an identity thief can leverage. Digital devices, mail and trash are the usual places from where personal details can be obtained easily.

Insecure Online Data: The digital era has brought bountiful conveniences, from making purchases online to viewing accounts and paying bills with the click of a mouse. Our increasingly paperless lives may be seen as lowering the risks of off-line causes of identity theft such as stolen mail or trash they also render us to the new and more vulnerable processes of identity theft. A few examples in which data can be reached online are, unsafe connections, insecure websites, password security, phishing and doxing.

Company-Wide Data Breaches: Amongst the noted causes of identity theft, data breaches emerge out completely as they tend to have rapid impact on a massive group of people. At the most fundamental level, a data breach occurs when some sort of secure information gets leaked either through a suspicious act or by accident into a risky Apart from credit card numbers, a data breach may also leak victims' email addresses, passwords, social security numbers, and even those of the victims' family members.

Now-a-days, identity theft has become a common concept describing online thefts. It's been happening around since time began, but it has taken an entirely new dimension in the age of technology where people

can do personal business remotely from a computer without even actually having a face-to-face interaction with each client or a dealer. As explained, identity theft takes place when an unknown or even known person to the individual pretends to be the latter. In and of itself, this is a crime, but when the thief also uses your identity for personal gain, it aggregates the offense. It's not necessary that all the victim's personal possessions may have been captivated; there may be a large and serious number of for victims. If the criminal has used another person's identity to commit a crime, there may be a case which brings the victim under police suspicion. The victim may find themselves being investigated for criminal investigation, and in some cases, they may find it difficult to prove their innocence. People who are the victims of financial fraud have to face ample number of issues. If a person uses personal details in any form of monetary transaction, one could end up being overloaded with debts. In most cases, if one can prove that the debts are not their responsibility anymore, consequently they are not liable for them. On the other hand, however, it can also be very difficult to prove that they are not at fault. Whilst credit agencies are supposed to remove incorrect information, they take a longer period of time for doing so. By the time that the information has been updated, one may have already been rejected for al number of credit opportunities. A credit check done on the victim in future will then see these rejections, and this may affect their credit decisions. A few people even face trouble in getting a new phone contract once they have a black mark on their credit rating. Most credit agencies will put a notice of corrections on to the credit file, but people who are doing a quick credit check may not even notice this. It is therefore important to spot identity theft as early as possible and it varies from person to person. Victims of identity theft are rarely harmed physically unless the theft has come because of a mugging or similar physical robbery. If one is or was the victim of such a violent crime could have left psychologically or physically affected (or both) as a result. If this is the case, then a victim might fetch some amount of comfort in the knowledge that they could potentially make a criminal injury claim for compensation. In extreme cases, a criminal may even commit non-financial crimes in someone else's name, for which the victim must then suffer the consequences.

Problem statement: Most of the people across the globe are aware about cyber-crimes, but not many are aware about the identity theft based cyber-crimes. The present study is conducted to measure awareness of people about identity theft and its consequences while using internet

Literature Review: Swapan Purkait in his paper Phishing counter measures and their effectiveness discusses about how phishing has become a social engineering crime on the web. The techniques are becoming and posing big challenges for researchers. The purpose of his study was to examine the literature and counter measures. [21]'Study on Phishing attacks and Anti-phishing tools' a research paper by Dr. Radha Damodaram explains how now-a-days, internet has a remarkable platform for people to communicate. The people with criminal mind found ways to steal personal information. It poses a great threat to electronic commerce industry. All this gives awareness about attacks and related anti-phishing tools. [3]James L. Parrish, Jr. Janet L. Bailey, James F. Courtney have written a research paper about A Personality Based Model for Determining Susceptibility to Phishing Attacks explaining about how phishing, which is a type of social engineering attacks to gain information by computer. The attacks started increasing on an alarm rate and causing damage to individuals and organizations. [15] K. Jansson and R. von Solms in their research work,: Phishing for phishing awareness' describe how using various social-engineering techniques, criminals run havoc on the Internet and defraud many people in a number of

different ways. This puts various organizational communities at risk. [16] A survey of research on context-aware homes', written by Sven Meyer focuses on the integration of people and how devices & computation become part of people's daily life. Wireless networks blend into future environment. Technologies are often replaced according to the needs of the user. The paper presented research on issues that enhance the quality of life to creating hacking awareness. [20] Mikko T. Spinonen in his research named A conceptual foundation for organizational information security awareness' highlights the current approaches of information security awareness and education is descriptive. The current research has not explored the possibilities offered by the motivation. The role of motivation in information security is not considered seriously; the role has been widely recognized. The security awareness and education will analyse from viewpoint on their strengths and weakness. [19] Ethical Hacking' a research paper written by C. C. Palmer illustrates how the growth of interest brought many good things electronic commerce, easy access to vast stores, collaborative computing, e-mail, advertising & information to name a few. Due to technologies advances, there are criminal hacker, government companies, and private citizens are anxious to part of revolution. But they are afraid about hacker break web server & credit cards from online sites. The ethical hacking is explained, global security analyses the problems. [2] Tamala Adam Lerner, Adam Shostack in their paper Control- Alt-Hack: Design and evaluation of a card game for computer security awareness and education, create the designed, produced, tabletop card game created awareness & alter regarding computer security. The report on the feedback, about the experiences use of Ctrl-Alt hack, 22 of these educates about with 450 students in classrooms & non-classrooms contexts. 11 of them have increased awareness of computer security % furthermore, intended goals upon the responses. [22] Authors Ashish Gupta and Anil Dhami in their research paper 'measuring the impact of security, trust and privacy in information sharing: A Study on social networking sites", have mentioned that in internet in social networking websites have thrived. Computer mediated they have changed the communication with social networking like Facebook, Google+ and twitter, facilitate user features with online interactions, sharing their personal information raised to privacy concern. [1] Personal information sharing behaviour of University students via online social networks' a research paper by Ghulam Murtuza Rafique explains how with privacy concerns it is important to understand how university student protects their personal information. Any information can be distinguished and traced to an individual's identity such as name, social security number. The purpose of this study was to determine the personal information starting online social network. [5] Dr. Saswati Gangopadhyay and Ms Debarati Dhar in the paper Social networking sites and privacy issue concerns explains how social network is now allowing young users to mingle with larger network of known and unknown friends. It is addicted to youth people who create online profiles, hooked to mobile phones, laptops and PC's. This paper focuses how this privacy encourages the youth to measure and sharing personal information. [4] How much privacy we still have on social network written by authors Mafaisu Chewae, Sameer Hayikader, Muhammad Hairulnizam Hasan and Jamaludin Ibrahim, explain that how internet is one of the most efficient to communicate on the social networking Over billion users are connected through online social networks and share their personal information. In this paper we will study how personal information is being influenced by internet and how to employ security awareness to avoid privacy risk. [17] Zhou Cheng Zhang Bo, Li Qian Mu have written a research paper on the topic Research on Reduced Optimization of Illegal Access Information in Database Internal and external networks focuses on the research on optimization of illegal causes inside and outside improve the security of network database. The need to collect accurate data and repeated nuclear iteration, so that known access to linear distribution data can complete the information to restore. Proposed multi-core composite internal and external network illegal access to information collection accurate reduces method. The purposed method has strong and can improve security of internal and external network information. [23] Streaming and online access to content

and services, by Mariusz Maciejewski, Nina Isabel Caroline Fischer, Yana Roginska described the situation where in even though internet is increasingly offering an interactive or appearing - access to content, this improved access is, leading to more quality, innovation and a significant reduction of the environmental footprint through dematerialization of consumption, with potential changes in the economic and societal landscape. However, the current legal and economic setting in Europe is leading to a partitioning of mobile Internet access and Internet content along national borders. [18]

Experiment Conducted and the Results: Authors have conducted a survey of some people of various age groups and genders from Mumbai region who are using internet for various purposes. The questionnaire is prepared to cover questions on sharing personal details, using public wi-fi facilities, awareness of online scams, hacking and websites where they share their personal details. Microsoft Excel is used to compile responses and it is also used to analyse the data. Various charts are drawn to analyse the data.

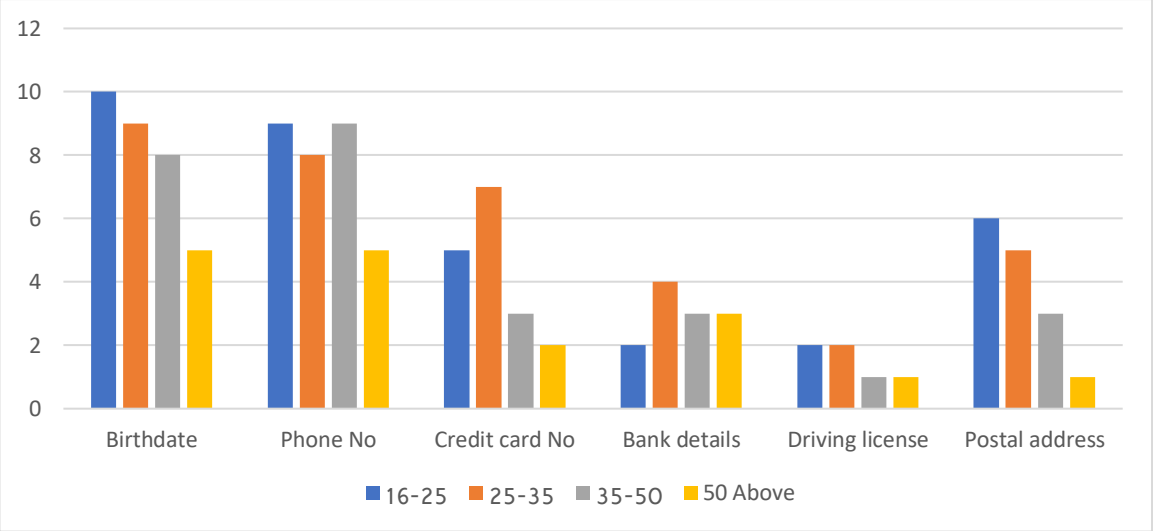


Fig 1: Personal details sharing

From figure 1 it is observed that, most of the people share their birthdates on various internet websites. All age-group people share their phone numbers most of the time.

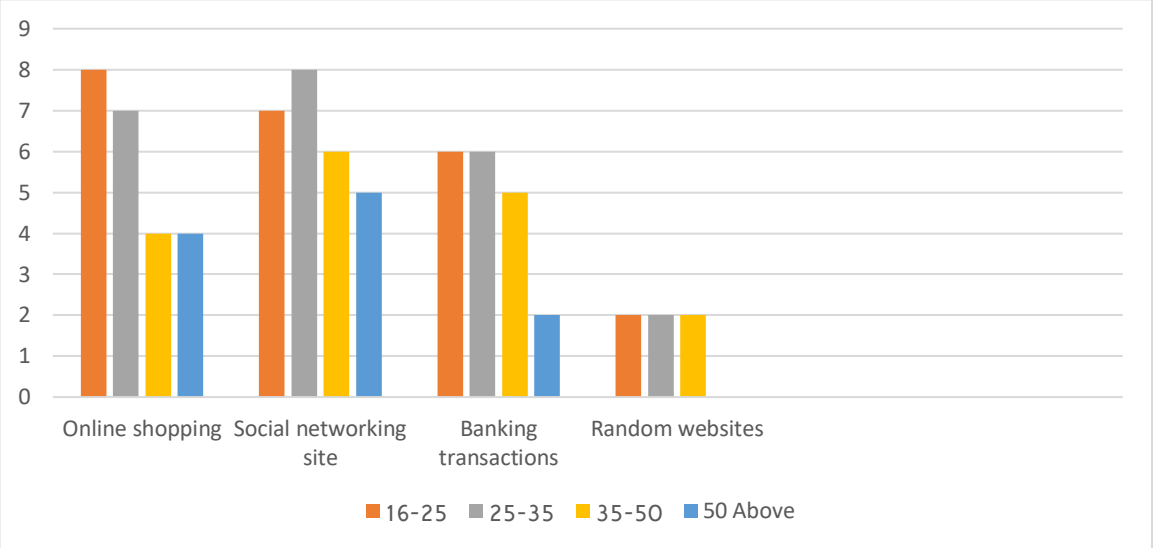


Figure 2: Places where personal details are shared

From figure 2 it is observed that, people belonging to age 50 and above do not share their details on any random websites

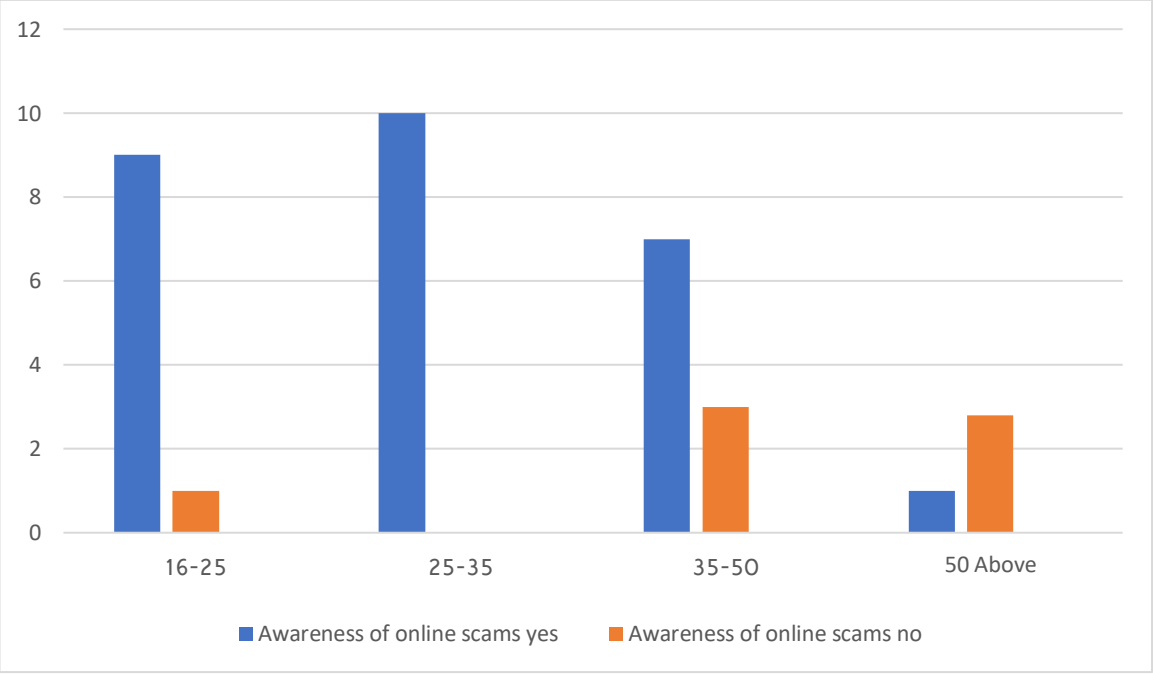


Figure 3: Awareness of online scams

From figure 3 it is observed that, none of the people belonging to age 25 to 35 are suck who are not aware of the online scams.

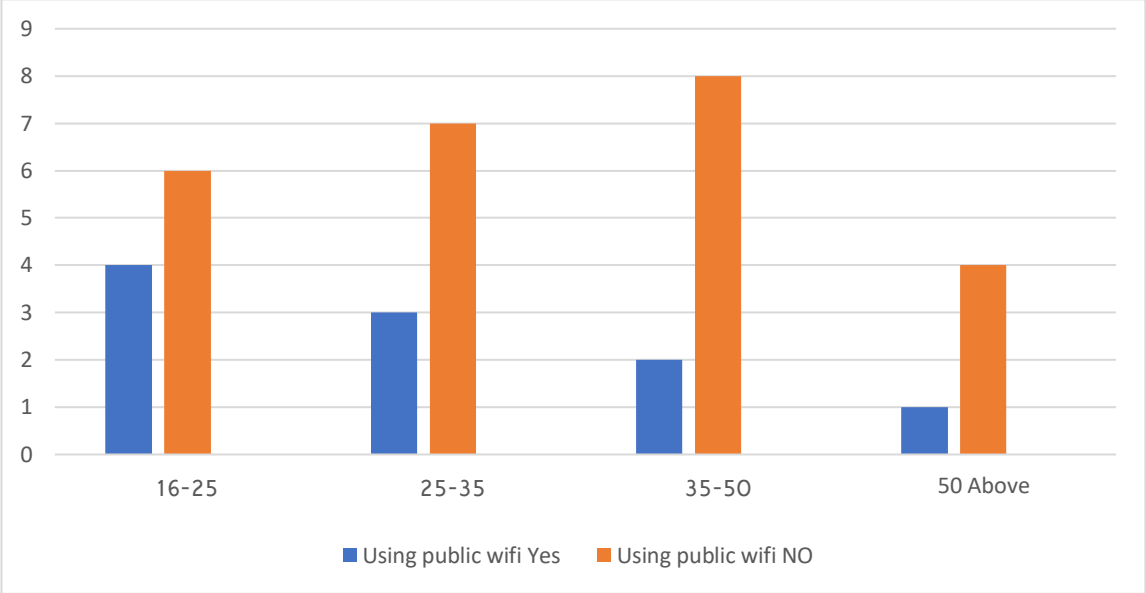


Figure 4: Using public wi-fi

From figure 4 it is observed that most people from 35 to 50 do not use public wi-fi.

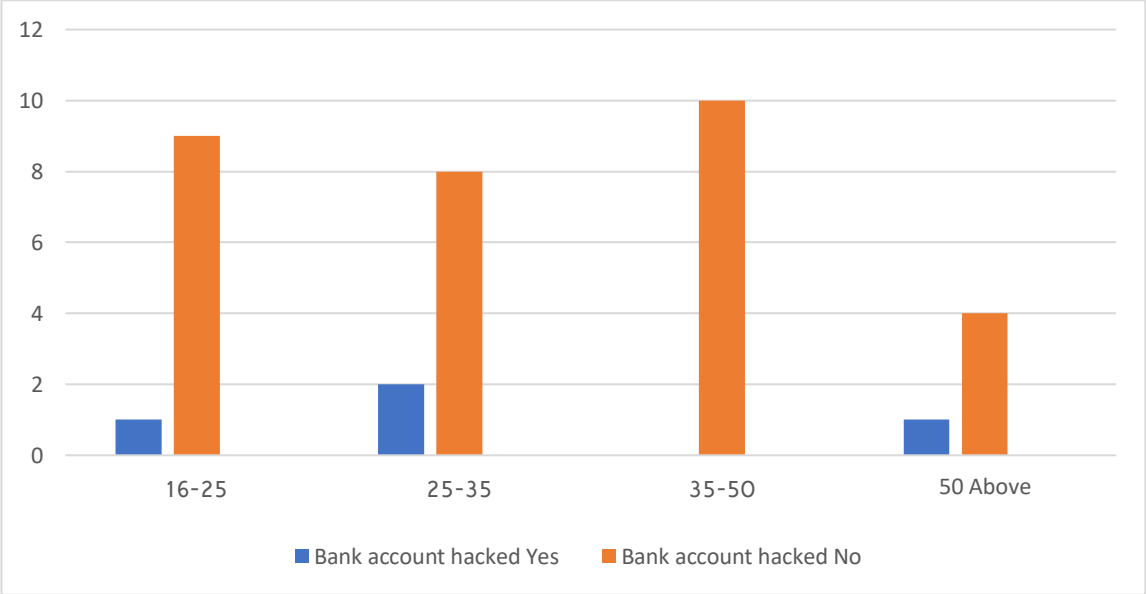


Figure 5: Bank account hacking

Form figure 5 it is observed that, people belonging to age-group 35 to 50, bank account has been hacked through various means

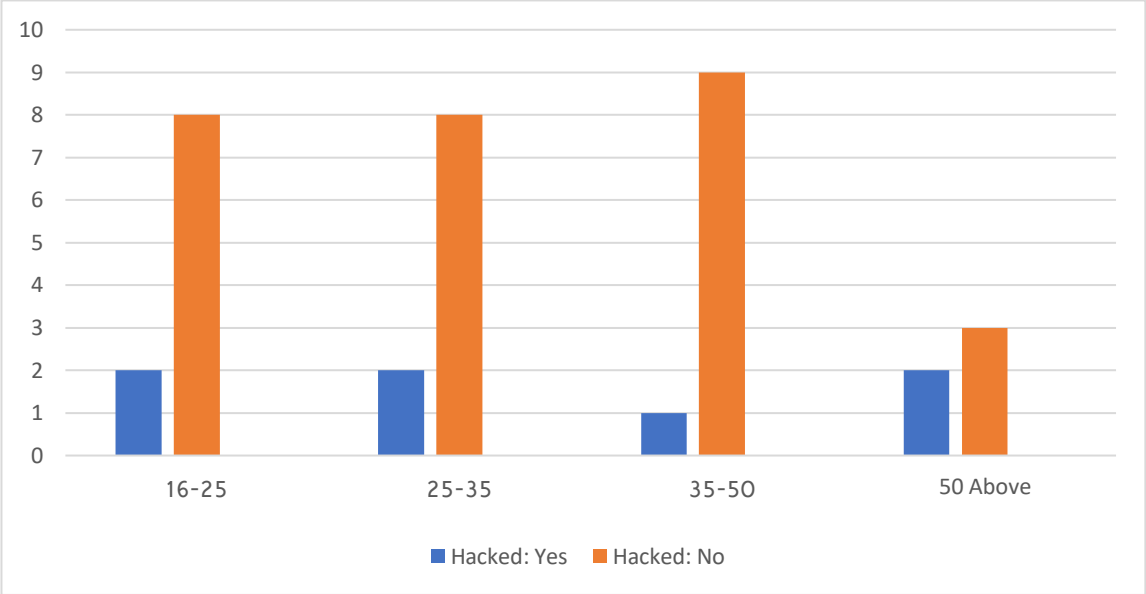
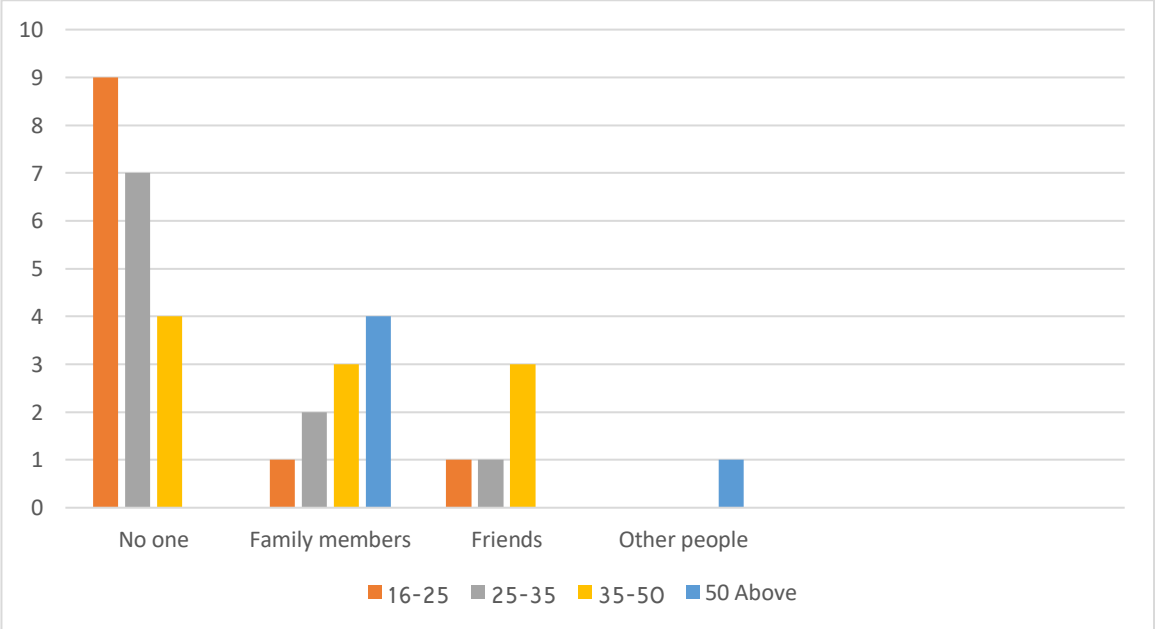


Figure 6: Social media account hacked

From figure 6 it is observed that people from 35 to 50 their social media account has not been hacked.



7: Sharing online account username and passwords

From figure 7, it is observed that people from age group 25 to 35 share their account and password with other people. Whereas except age group 50 other age groups do not share their password and accounts with other people,

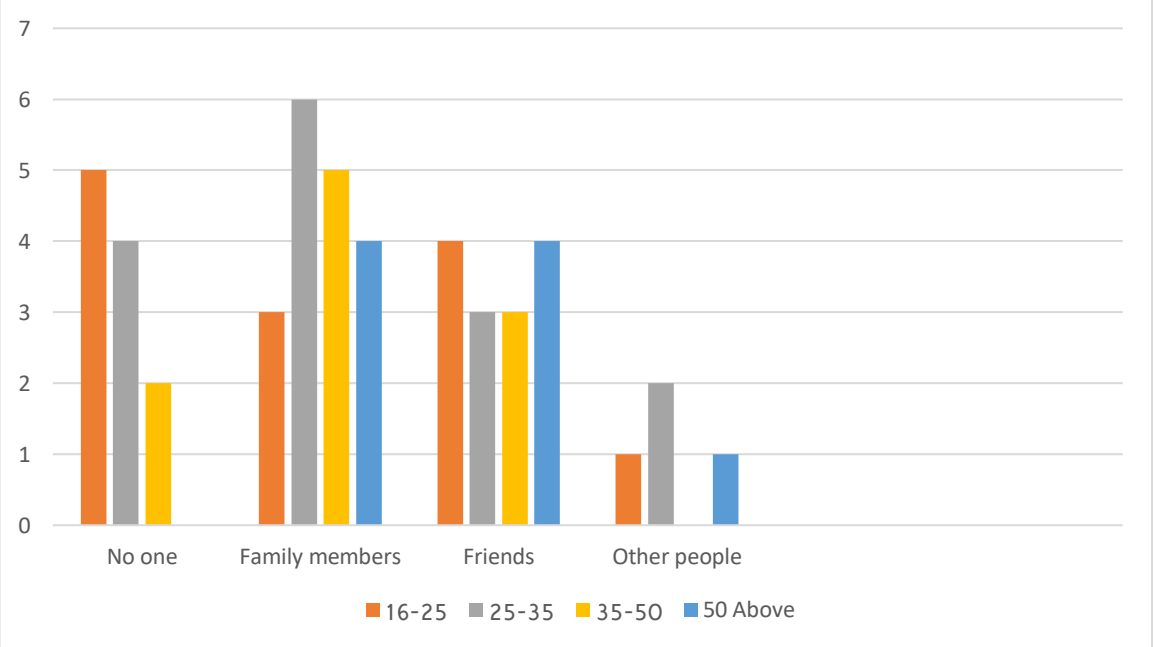


Figure 8: Sharing mobile handset passwords

From figure 8 it is observed that, most of the people from all age-groups share their mobile handset passwords with family members, followed by friends in the hierarchy seen in above figure 8.

We are mostly used computers and mobiles for browsing from internet. There is some software and technique we should use to prevent online fraud with us.

Anti-virus software – We should use and install anti-virus application or software to keep safe our system or machine or computer from malware or any type of virus. Most of viruses comes using internet while clicking any fraud links etc. So if we are having such software installed in computer then it will help to prevent such fraud. Some anti-virus software's are McAfee, MalwareByte.

Keep your system updated – we should keep our system up to date so new patches will install and help us to prevents attacks.

Keep firewall on – We should on firewall setting in out computer that will help to prevents attack and fraud.

Don't share any one-time password(OTP) with anyone.

Don't share your banking or any personal account password with anyone.

Use required application or software.

Don't provide all permission while accessing any app from mobile. Example: If you have installed any camera application so that app is not required your contact, SMS access permission. You can check all application permission in your phone using application settings option.

Make sure your mobile or computer is up to date with latest update and patches. Frequently antivirus scanning is also recommended.

Don't save your password in mobile software such as notes or any application. Many times, our data that stored in app such as a password, the owner or developer can breach our data. Don't use such application those uses internet to store data. It is safe if our data stored in our mobile device locally without internet.

I have created android application to save our data in our own device without internet. This is safe technique to store our data locally so no one can access that data from internet using hack.

Here is the link of the application, you can download the app and install in your phone.

https://github.com/Krasam/PasswordSafe.git

Conclusion: From the study it is observed that, many of the people are aware of online scams occurring in our day-to-day life. Public wi-fi connections are majorly used by the young generation age group 16-25. Also, social media sites such as Facebook have been hacked most of the times and have occurred mostly in the age group 16-25. The reason behind it might be sharing password with friends and other people. WhatsApp account has not been hacked even once, according to the analysis performed using the statistics done on the collected data. People belonging to the age group 25 to 35 are observed sharing personal details like birthdates and phone numbers over the social networking sites, which is highest among all the other age-groups. The age group above 50 share details using social media the least. Other than the mentioned social media accounts, one of the individuals has also reported hacking about a popular professional social media application called LinkedIn. To avoid identity theft based cyber-crimes, online websites users must be very alert while sharing personal or professional information.

References:

Ashish Gupta and Anil Dhami. 'Measuring the impact of security, trust and privacy in information sharing; A Study on social networking sites', Macmillan Publishers Ltd [Journal of Direct Data and Digital Marketing Practice], Volume 17, Issue 1, pp 43-53

C.C. Palmer, Ethical Hacking, IBM System Journal, Volume 40 Issue 3, March 2001 Pages 769-780

Dr. Radha Damodarum, 'Study on Phishing attacks and Anti-phishing tools', International Research Journal of Engineering and Technology, Volume: 03 Issue: 01 Jan-2016

Dr. Saswati Gangopadhyay and Ms Debarati Dhar, Social networking sites and privacy issue concerns, Global Media Journal-Indian Edition, vol5 No 1

Ghulam Murtuza Rafique, Personal information sharing behavior of University students via online social networks. Libraries at University of Nebraska - Lincoln

https://www.acorn.gov.au/learn-about-cybercrime

https://www.acorn.gov.au/learn-about-cybercrime/attacks-computer-systems

https://www.britannica.com/topic/cybercrime

https://www.byte-notes.com/what-cyber crime

https://www.identitytheft.org.uk

https://searchsecurity.techtarget.com/definition/identity-theft

http://www.shareyouressays.com essays/short-essay-on-cyber-crimex-298-words/121700
http://www.shareyouressays.com/example-essays/505-words-of-essay-on-cyber-crime-in-india/1794

https:/www.trueidentity.com/identity-theft-resource /how-it-happens

James L. Parrish, Jr. Janet L. Bailey, James F. Courtney, 'A Personality Based Model for Determining Susceptibility to Phishing Attacks' Oklahoma City, OK: Southwest Decision Sciences Institute.