eISSN 2583-6986

IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Vol. 02, Issue 12, Dec 2022

Better Safe Than Sorry

[1]Mrs. Neelam Kanojia

[1]Assistant Professor Commerce, Government Degree College, Haripur Nishastha, Rae Bareli, UP

Abstract

A report published by McAfee," cyberbullying in plain sight" states that in India every one child out of five have reported of receiving online threat. Experiences like these take a hugetoll on the wellbeing of child. Thus, it has become crucial to take in account such incidents. Every now and then we hear distressing news of somebody getting duped of money curtesy to online scam or disappearance of people who ran away to meet their online friend. Relinquishingtechnology is not a viable option when it comes to tackling technology, a better option is to develop a prophylaxis to create a healthy relationship with the electronic world. This paper aims to create awareness of the online threats and tries to provide guidance to safeguard from online threats.

Keywords: cyber-bullying ,phishing, cookie theft, cybercrime.

Introduction

Digital Technology is a double-edged sword .one must use it wisely in order to reap its benefits. today it is nearly impossible to imagine world without the use of technology.it has spread its arms across all the domains. The arrival of covid forced many changes in the way we live.one such change is the hybrid mode of learning where education is provided using two mediumsvis a vis physical classroom and other is the online mode. According to TRAI Report (2021), data usage in India has increased 43 times in last six years. digital growth is expected to riseby 28.6% annually till the year 2024.such statistics proves that digital market is growing by leaps and bound day by day. Digital technology is everywhere. It has impacted as to what, when, why, how, where and from whom the students are learning. Whatever information is put into the virtual place is difficult to delete more or less it is permanent. The transmission of message be it authentic of false is at lightning speed. Therefore, it has become very importantto make users understand to validate and check information as spreading of false news as true news leads to unnecessary panic and occurrence of untoward incidents. Needless to say, this that digital technology has its pros and cons one must use it with caution or may have to suffer a great damage.

Digital technology forms like internet, tablets, laptops are used by numerous educational institutions like schools, colleges etc. these provides plethora of benefits like are easy accessto vast resources, quick, personalized learning is possible, cost effective and so on. having said that digital technology also poses serious threats. A continuous upgradation in technology creates a new learning atmosphere for the young adults thereby effectively increasing gap between the generation, be it predecessor or successor. Due to this incessant growth in this arena parents and teachers find it difficult to keep up with the younger generation. Precautionis always better than cure.to safeguard ourselves from the various types of threat that cyber activities poses.

Parents and teachers were jolted by the news of the sudden death of fourteen-year-old boy who jumped off the terrace to complete a blue whale challenge, an online suicide game comprisingof

fifty gruesome tasks which they have to document it. the challenge concludes with the final task where the player has to end his life. Such unfortunate instances show us the vulnerability and the extent of danger internet poses to our children. young adults with limited experience and their trusting nature often are soft target to person with malevolent nature. in a space where the children are bombarded with information it is thus become vital to make them aware of all the aspects of the information; the technical know-how the technology, the threat it poses and the measures to safeguard from the threat We must first understand the several types of risks associated with the technology. Some of the cyber-attacks are discussed below:

Key logging: One often uses the keys of keyboard or touch pad of and electronic device to type in the information to get the desired result. A person with malicious/hacker intent may install a software app or a physical hardware in the device to track the information in the device the "app" would store the data and provide it to the hacker. recording of key strokes would give access of the password, financial information and personal information of an individual to the hacker to misuse as and when he pleases.

Denial of service (Dos): assume a scenario where you are highly waiting for a sale on a certain website and on the day of sale you are not able to visit the site or purchased the desired item that you were longing for due to server being down as there are vast numbers of customers trying to buy which leads to heavy traffic on the server. When denial of service attack occurs similar types of traffic are logged into the server resulting the costumer not being able to use the service provided by the genuine websites of the organization.as this often causes the websiteto become unstable and it freezes or hangs.

Phishing attack: you might have heard an incident where an individual has won the lottery and instead of gaining money, he ended losing his bank balance. This is an example of phishing attack whereby the attacker uses any mode of communication to make you reveal the confidential information which are not be shared under circumstances. the attacker may send fraudulent messages laced with virus or trojan that appear to be genuine through emails or any such communication modes. here the victim is made to believe that the messages are sent to them by a trusted sender and are often coaxed to share their confidential information on fake website of the trusted organization. Invariably when the attacker gains access to such information uses to steal money or launch other attacks

Waterhole attack: it is an attack where the predator targets the websites/service which the victim is most likely to visit for example a free Wi-Fi in public place. then the attackers initiatea chain of events by creating fake Wi-Fi access point or compromise the website inadvertently the victim ends giving entry to the attacker in his computer network. where the attacker can easily manipulate the information as when he pleases.

Eavesdropping: Mostly in communication model the sender encrypts a data to an intended receiver. If the data /message is intentionally decoded by a person other than the intended receiver without the knowledge of the sender this occurrence is known as eavesdropping. The attacker is able to intercept the information between the devices like laptop and mobile phones with microphones and use it for malicious purpose. Eavesdropping can be used by the perpetrators for financial gain, identity theft and to invade privacy of the victim.

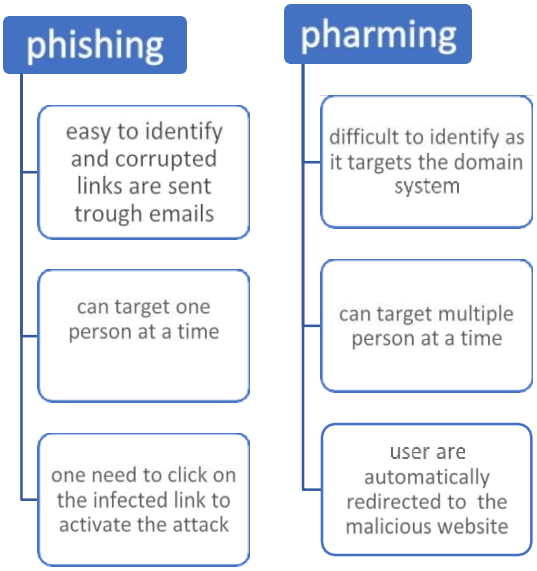
eISSN 2583-6986

IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Vol. 02, Issue 12, Dec 2022

Pharming: When a server is trying to log into a website but instead, he is directed to another malicious website this activity is called pharming, where the users are directed to website other than the intended website. Mostly such types of attacks are often seen in banking and e- commerce sites. The goal is to obtain personal information like credit/debit cards details, passwords and so on to commit financial fraud or identity theft.

Difference between phishing and pharming.

There is a always a confusion between phishing and pharming as both try to get the victim to share the information used to commit fraud be it financial or identity. The difference between the two is that phishing involves use of communication channels like emails and SMS to send the infected link whereas pharming involves a deeper study into the domain system which redirects the users to the fraud website.



Clickjacking: also known as user interface redressing. In this technique of hacking the attacker lures the victim into clicking to what is visible to them on screen but in reality, the option is hidden with a different user interface through which the attacker steals the data. For example, Mr. A visits a website where the page appeals him to avail a free smart phone intrigued by this offer Mr. A decides to avail this offer and clicks the option of avail now. Here Mr. A thinks thathe is availing a free smart phone but in reality he has clicked the option payment transfer which was hidden from Mr. A. All the details of Mr. A bank details has been hidden by the website. Which results in Mr. A losing his bank balance rather than getting a free smart phone.

Cookie theft: Cookie is small pieces of data which stores information user name passwords which are used to identify the user through the respective computer. Cookies are designed to enhance the browsing experience by identifying the user's preference. For better understanding, suppose a person is shopping on an ecommerce site cookies will help to recognize the user and hence he does not require to log-in every time he opens the site and displays the users preferred information.it also remembers the information feed in so that the users do not require to feed information again

eISSN 2583-6986

IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Vol. 02, Issue 12, Dec 2022

and again. Cookie theft is a type of identity theft where the hacker pretends to be the user using his cookies to log into the system.

Man in the middle attack: In a normal flow of network there are two parties, mostly they are the user and the server but in man in the middle attack the intruder positions itself between the devices of user and server and can efficiently manipulate or intercept the data. By using this technique, the intruder may pose as bank official and send message to a client to send his confidential information.

Spyware: While surfing on the net you may come across a pop up on your screen notifying that your phone is under threat of virus attack,9 viruses found to remove these viruses install this particular app. this type of activity is an example of spyware attack. Spyware is a malware that is installed in a device without the knowledge of the user to collect the information to assist a financial fraud or for personal gain.

Apart from the above-mentioned attacks cyber bullying is also a type of a punishable crime.

What is cyber bullying?

When an individual targets a person using digital technology with a view of harassing/tormenting him is called cyber bullying.it is a repeated attempt to embarrass, instigate or scare the victim.

- **Forms of cyberbullying:**
  - Spreading false information
  - Posting embarrassing photographs/videos on social media
  - Sending threatening, abusive and hurtful messages
  - Blackmailing
  - Impersonating as someone and sending mean messages to others creating conflict between the two.

Few precautions that can be taken to safeguard ourselves from cyberthreat: -

- Never share your password with anyone under any circumstances.
- Change your password within every 6months or year.
- Make sure your password is a combination of upper-case, lower-case numerals and special character.
- Do not open mails from strange email address, or click on suspicious link or sites.
- Cover your webcam when not in use.
- Always download app from a trusted app store.
- Disable location setting from social media sites and apps when not in use.
- Check the spelling of the address emails and messages from scam sites have a high probability of spell errors.
- Check the website address if it has **http** instead of **https** chances are high that it is a scam website.

eISSN 2583-6986

IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Vol. 02, Issue 12, Dec 2022

Install an anti-virus software and regularly update your browser.

- Be careful while accepting request of strangers. if you do not know person personally avoid accepting the request.
- Beware of fake social media account.
- Log out from the social media account when not in use.
- Block the person who makes you uncomfortable.
- Never keep quite, speak up. Talk to your parents or someone you trust if you facing such problem.
- If you feel uncomfortable/scared seeing any content take a screenshot and collect evidence and talk to your trusted elders and file a complaint at (www.cybercrime.gov.in)
- Never hesitate to take help from your near and dear ones.
- Do not blame yourself if you facing such acts of bullying
- Help your friends don't be a silent observer if you are aware that your friend is being bullied.
- Try not to react when someone is trying to bully you instead, keep a record and reportit to the concerned authorities.
- If a person asks you to keep the conversation private and not to share it with any one there is a high chance that the person asking you to do so is shady individual.
- Report a stolen/lost device immediately and block your accounts.
- Always do a background check/verify before posting/spreading any information. Find the source of information.
- Never try to meet a person who you have met online.
- If you are a victim financial fraud, immediately call the helpline number 1930 and register your complain www.cybercrime.gov.in

Conclusion- The cases of online frauds and mishaps are increasing day by day. scammers often target the naïve users on net to accomplish their selfish motives as the result the unsuspecting users easily fall into the trap of such scammers. Thus, it has become very important to educate the citizens about the risks and modus operandi of such hackers so that they do not fall prey to these tactics.one must be aware of the menace that online surfing has and take necessary precautions against it.so that one can utilize the technology at the optimum level for the betterment of self and country.in the view of rising online fraud in the country ,the ministry of home affairs have launched a portal and a twitter handle "cyberdost" to protect and educate its citizen. This portal also helps the victims to register their cases of online fraud or harassment. Technology is an essential part of education hence we should not be afraid of the threat and abandon the technology instead we must adopt and avail technology with utmost care and vigilance.

eISSN 2583-6986

IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Vol. 02, Issue 12, Dec 2022

Bibliography:-

1- Hall, G., & Watson, E. (2016). Hacking: Guide to Basic Security, Penetration Testing and
   a. . Retrieved from https://mogami.neocities.org/files/hacking.pdf
2- What is Keystroke Logging and Keyloggers? (2022, May 12). www.kaspersky.co.in. https://www.kaspersky.co.in/resource-center/definitions/keylogger
3- Denial of Service (DoS) guidance. (n.d.). https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection
4- What Is a Phishing Attack? Definition and Types. (2023, March 22). Cisco. https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html
5- CSRC Content Editor. (n.d.). watering hole attack - Glossary | CSRC. https://csrc.nist.gov/glossary/term/watering_hole_attack
6- Wright, G., & Bacon, M. (2021). watering hole attack. Security. https://www.techtarget.com/searchsecurity/definition/watering-hole-attack
7- Awan, H. (n.d.). Eavesdropping Attack: What Is It, Types, Its Impact, and PreventionTips. https://www.efani.com/blog/eavesdropping-attack
8- What is a pharming attack? An overview + prevention tips. (n.d.). https://us.norton.com/blog/online-scams/pharming-attack#
9- Sengupta, S. (2022, September 12). 【Clickjacking Prevention 】What is this attackand Examples. Crashtest Security. https://crashtest-security.com/clickjacking-attack/
10- NordVPN. (2023, March 7). Cookie theft. https://nordvpn.com/cybersecurity/glossary/cookie-theft/
11- What Is Spyware? Definition, Types And Protection | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/spyware#:~:text=Spyware%20is%20malicious%20software%20that,device%20without%20the%20user's%20consent.
12- What are Cookies? (2022, May 11). www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/cookies
13- Government of India,Ministry of Home affairs, https://cybercrime.gov.in/webform/FAQ.aspx