Cybersecurity: Issues and Challenges

G P Pandey

Humans are the weakest link in cyber security chain. Amateurs hack systems but professionals hack people. It has become imperative to create awareness in the use of digital platforms through digital literacy. It is an essential requirement for safe and secured use of digital resources.

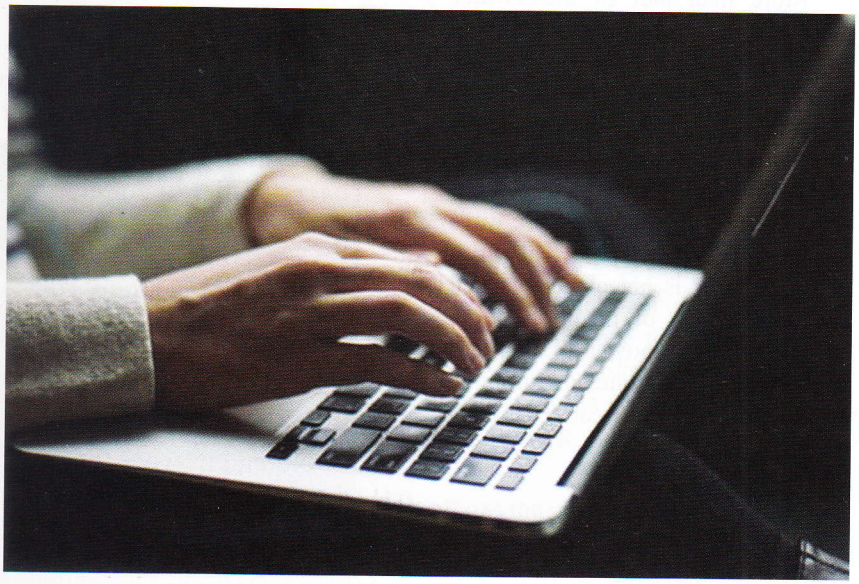
The world we live in is highly connected and digitally exhaustive. Of the 7.6 billion humans on earth, around 3.6 billion are online. Today, social networks have become one of the main communication channels. Within relatively short time social media has empowered people and connected them. But, at the same time, they have also provided platforms for some decidedly unhealthy and destructive behaviour. Social media platforms have become just one of the endless data channels that cybercriminals are exploiting.

In this era we need skills for surviving in digital environment. For security and safe use of digital resources, digital literacy has become a must. It empowers us with the ability to use information and communication technologies to find, evaluate, create and communicate information requiring both cognitive and technical skills. Digital natives are always with laptops or smart devices in their hand, but how effectively they are using internet for their capacity building is questionable. There are many problems like bullying, cyber crime, copyright issues, security threat and social unawareness among others. Digitally literate individuals find meaning in digital information and make use of it; they exhibit the characteristics of cultural and social understanding, collaboration, the ability to find and select information, effective communication, E-safety, functional skills, creativity and critical thinking. Therefore, to avoid and prevent threats in digital world, digital literacy is essential, which helps in creating awareness in digital space.

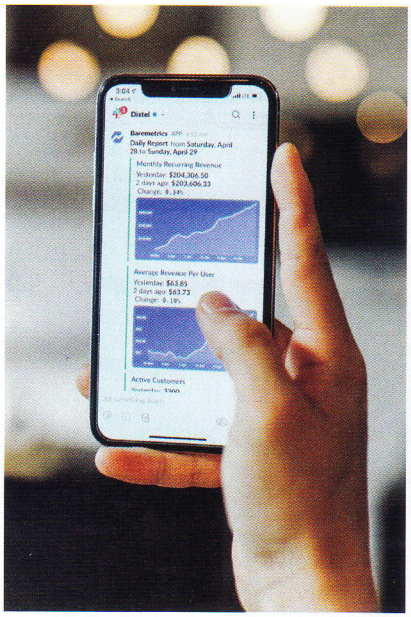
In the year 2016, there were a total of 758 million online attacks worldwide, which amounts to around 2 million in a single day. Even technically legal activities often involve misuse of individuals' Personally Identifiable Information (PII). Every organisation, be it big or small, has been the victim of cyber attacks. This reiterates that cyber attacks are real and your and my account can fall prey to it, counting on any random day. Therefore, it is required to create awareness on learning to mitigate the attacks.

Bots

Bots and fake followers are a big concern in the social media environment. Bot programs target specific hashtags and work by auto-commenting and auto-liking in order



The author is Professor and Dean, Abanindranath Tagore School of Creative Arts and Communication Studies, Assam Central University, Silchar, Assam. Email: gpp59aus@gmail.com



to attract followers who are mostly other fake bot accounts. These are automated systems which can on their own get engaged with other users without any active presence. Developed primarily for companies to engage with their users automatically for increasing customer engagement, bots are now being used much beyond their harmless cause and are misused for manipulating a conversation to creating a mirage of someone's personality and much more.

More than half of the Twitter followers of many public figures around the world were found to be fake.[1] Companies are addressing the issue by suspending fake accounts. But the problem persists. We do not know if a 'like' is generated by a bot or a real user. Though there are ways to differentiate between a real and a fake profile, it is not always carried out. In this age of misinformation, bots possess the power to hijack a conversation, troll someone, promote propaganda and even cause security issues.

Terrorist Attacks

Terrorists have always sought attention and that is what they receive from the social media. Whenever there is any terror attack, as a response to the horrific events, people share images and videos of the devastating attack on social media. Social media thus spread the horror far and wide and unknowingly amplify the chaos that the terrorists intend to spread. In the process, misinformation and fear spread. It further traumatises the families of the victims and also the public at large.

Extremists use the social media to make an impact. They even use it to recruit, propagate and to connect. Moreover, they rely on the regular social media users to spread the impact of terror further to a greater degree than what they themselves could have done in addition to confusing authorities with misinformation.

Misinformation, the rapid spread of false information through social media is among the emerging risks identified in Global Risks Report. Fake news and rumours spread like wildfire in the social media and it is also increasingly used for militancy.

Social media sites have now initiated reporting procedures that allow users to flag any kind of content that supports terrorism which can be then removed. Also, the social networking sites today are playing an important role in counter-terrorism operations. The law enforcement authorities make good use of the social media by keeping people informed regularly. For example, Assam State Police opened a cell to monitor social media and keep track of the spread of rumours.

Digitally literate individuals find meaning in digital information and make use of it; they exhibit the characteristics of cultural and social understanding, collaboration, the ability to find and select information, effective communication, E-safety, functional skills, creativity and critical thinking. To avoid and prevent threats in digital world, digital literacy is essential, which helps in creating awareness in digital space.

Cyber Security Challenges

Some new threats have also come up like organised cyber crime, cyber crime trading, smishing (phishing with SMS), hacktivism (hacker with activism) etc. Another type of attack that is rising recently is distributed denial of service (DDoS) attacks. Here the intruder is not interested in actually stealing your information but in bombarding your server with unnecessary traffic thereby crashing it. Huge servers like video streaming apps and majority of banks are under this type of attack. Any device that can connect to the internet can be breached. If an individual by mistake clicks on a link that contains malware or accidentally discloses sensitive information, their accounts get exposed to hackers, cybercriminals and identity thieves.

Mobile Technologies

Not only are we living in a highly connected world but also in a world that is highly mobile, given the amazing number of apps that we use on a daily basis. Have you ever wondered how many sensors are there in your smartphone and what type of personal information are they collecting?

Accelerometer, microphone, camera, location, contacts, gyroscope (for orientation), heart rate, proximity, light, temperature, pressure, barometer (for altitude) are some of the information that are collected from your phone. All the apps that you use let your smartphone know who you are, where you are, where you have been, who you know, where the people you now currently are, what you bought, where you bought, what you ate, whether you went and

even your current mood! But the more important question is who is it sharing the information with? When you download third-party apps, are you really aware that you are giving away the rights to collect your information? If your fitness app needs access to your text messages, that doesn't sound right, does it? What if a hacker is able to build your digital profile by collecting all these sensored information and the data from the third-party apps and use it against you?

A popular third-party app recently disclosed a data breach that compromised all of its 4.7 million users' email addresses and phone numbers. This data can be used to execute large-scale phishing attacks meant to compromise a company's network and systems.

Internet of Things (IoTs) is another such challenge posed by the new technology whereby every object we use is equipped with the capabilities to identify, locate, sense its surroundings, compute and communicate. Now what will happen if all these objects could talk to each other and share information? It is said that soon there will be one billion IOT devices and they will all be talking to each other. Imagine what a rich attack surface it is going to give the hacker and the number of attacks that can happen with IOT devices.

It has become imperative to create awareness in the use of digital platforms through digital literacy. Digital literacy is an essential requirement for safe and secured use of digital resources which can contribute to efficiently tackle the cyberspace.

Ransomware

This ransom demanding malware is a virus which gets into your computer, either when you download an attachment containing the virus or when you visit any such website and click on a link. Once it gets into your computer, it starts to encrypt all your files thereby rendering them useless. The only way to unlock your files is to get a secret key from the hacker by paying a ransom. And this ransom is usually demanded through bitcoin which keeps the payee anonymous. There has been a 600% increase in ransomware variants since 2016. Major universities, hospitals, businesses and even individuals have been target of such attacks.

Big Data

We are actually living in exponential data times. In just 60 seconds 149,513 emails can be sent, 3.3 million FB posts can be made, 3.8 million Google searches can be performed, 500 hours of YouTube videos can be uploaded, 29 million WhatsApp messages can be sent and 448,800 Tweets can be made and millions of other online activities can be performed leaving incredibly large digital footprint.

Unfortunately, humans are the weakest link in cyber security chain. Amateurs hack systems but professionals hack people. It is way easier to con people using social engineering techniques and make them reveal information rather than using tools and technology. The weakest link happens to be our password with which social accounts, mail accounts and millions of bank accounts have been hacked. An analysis of 32 million breached accounts has revealed that people most often use insecure passwords.

While all these makes the cyberspace a huge threat in the socio-economic environment of the present times, it has become imperative to create awareness in the use of digital platforms through digital literacy. Digital literacy is an essential requirement for safe and secured use of digital resources which can contribute to efficiently tackle the cyberspace.

Today, the Government is increasingly going for a digital system for more transparency. When we welcome development, insecurities come with it and tackling such insecurities is the main concern.

Protection against Cyber Attacks

As the channels and networks for data sharing continue to evolve and grow, so do the risks. For securing information on the social networking sites, following guidelines can be followed:

1. Limit the amount of information that you disclose on the social networking sites;
2. Do not establish friendship with strangers;

3. Do not believe online information blindly as it can be misleading;
4. Customise your system settings according to your needs by changing the default settings. Learn how to use privacy settings on your social profiles properly;
5. Beware of third-party applications. Avoid applications that seem suspicious, and make sure to modify your settings to limit the amount of information which the applications can access;
6. Secure your system, because unsecured network can lead to loss of your personal data;
7. Use antivirus software to secure your computers and electronic devices;
8. Use strong passwords to protect your account and personal information. Change your passwords frequently;
9. Do not set the same password for all social accounts, because if one site's password is compromised, all other accounts will be exposed to threats;
10. Choose suitable authentication scheme so that no one can access the details. Two-factor and multi-factor authentication should be in place. In two-factor authentication along with username and password, another form of identification, often a security code in the form of a "*Captcha*", is used. In multi-factor authentication, more than one form of authentication to verify an identity is used. Some examples are facial recognition, iris recognition, voice ID and finger scanning.

Today's digital world necessitates people to know the network security implications and spot suspicious activities. Oversharing helps hackers steal PII and sell it to the dark web.

Conclusion

Digital literacy is a broader concept that consists of developing new skills and knowledge which provides awareness and advanced level thinking skills. It is extremely essential to be digitally literate for appropriate utilisation of digital information resources. Therefore, it is the responsibility of each one of us to understand and help others to understand and use the cyberspace sensibly and responsibly. This will definitely ensure that the netizens are not only techno-savvy and socially existent but also digitally safe. ❑

Reference

1. Twiplomacy Study: https://twiplomacy.com/