P. WILSON Cyber Society of India Webinar – Inaugural Speech ON 5.6.2021

GOOD MORNING TO YOU ALL

I Thank Mr Balu Swaminathan President and Mr VN Prem Anand Secretary Cyber Society of India (CySI) for giving me this opportunity to give my inaugural address on this Sixth Kanni ni nar Series on **"Social Engineering, the Art of Deception"**

I have to say few words about CYBER SOCIETY OF INDIA. I am glad to say that it is working towards creating awareness on information security, cyber laws and related areas with a vision to contribute to the building of peaceful, ethical and prosperous Cyber netizen Society. CySI has conducted many workshops, conferences and seminars with participation from banks, IT companies, lawyers and Information Security professionals. CySI is focusing on creating awareness to professionals and general internet users towards safer internet using methodologies. Their mission is to provide a forum for debate, training, place of assistance and research, which actively promote good Cyber netizen Society and advise the concerned bodies on related matter.

Balu swaminathan as I know, was the made the first police officer to take care of cyber crimes by the Government of Tamilnadu. Many current police officers, judges seek his expert advise even today even after his retirement and his rich knowledge and exposure in cyber crimes help them to solve many crimes/assist to have a correct trajectory in this field.

Cysi has conducted various programmes, seminars and workshops relating to cyber risk, cyber laws, cyber security, cyber awareness etc since 2016 on the following topics

"Safeguarding Yourself from Cyber Risks".

"Workshop on Cyber Crimes: Guard yourself in the Cyber Space".

'Secur e-Banking'

Certificate course on Cyber Laws by CySI

“Handling Blue Whale like Threats”

Cyber Security and Challenges

‘Cyber Crime’.

Seminar on Cyber Crimes & Cyber Law

One Day workshop on Section 65 B of Indian Evidence
One day workshop on Digital Banking Awareness

Workshop on Personal Data Protection Bill was conducted by CySI jointly with Foundation of Data Protection Professionals in India (FDPPI) at Chennai in which I also participated. .

I am happy to note that CYSI is conducting this **KANININAR SERIES** - From May 2020 to till date and so far 5 Webinars on the topics like

1. How to Safeguard your Facebook account
2. Safe use of Mobile Phones
3. 65B- Indian Evidence Act
   (Sec. 65B - Admissibility of electronic records)
4. Phishing in the time of Covid19
5. Cyber Crime next to Identify Theft

Has been conducted.

Today, Cyber Society of India is conducting its 6th KANININAR (Webinar) Series on Social Engineering – The Art of Deception

What is SOCIAL ENGINEERING:

I am not thorough with the cyber knowledge. When I was asked to give inaugural speech on Social Engineering, I thought Social Engineering is associated some thing to do with uplifting of cyber technology. But after going through all the materials, I am shocked to know that “Social Engineering” is associated for all bad things relating to cyber frauds.

Social Engineering is nothing but Blue Print on cyber crimes. Its an Art of Deception in the arena of online technology.

Social Engineering is a way of collecting data and attacking the Information and Information Systems

Organizations and Individuals have suffered huge loss as a result of these attacks. However Social Engineering as a risk is neglected due to low awareness and absence of proper training for people.

I have come across many clients who have lost huge money due to this social engineering frauds. In fact we have filed several police complaints , but till today police are not able to make any break through on these frauds.

Few days back my face book account was duplicated and friend requests were sent to all my FB friends. After accepting the friend request, the fraudster started asking money saying that my wife is serious and that I require money. I got several calls and we laid a trap on him by seeking his bank details. The fraudster gave a mobile number for google pay and later we traced that he is in Utter Pradesh. But when I alerted the police the police gave me assistance and I am following that.

Friends even the Judges, doctors, engineers, and persons from various walks of life especially senior citizens have fallen prey for these frauds and have lost huge money.

Social Engineering based Attacks are the most common attack methods strategized by attackers. Exploiting the system and executing the malicious code needs proper understanding of vulnerabilities present in the system. However, the success rate of such technical attacks have been reduced by using technical controls. Therefore, hackers have currently adopted the alternative method – Social Engineering, exploiting the psychological vulnerability present in the individuals and potential technical vulnerabilities of varied technologies. Consequently, Social Engineering is now seen as the greatest security threat for people and organizations.

Socially-engineered attacks historically target individuals with an implied knowledge or access to sensitive information. According to a survey conducted for academic purpose, Hackers these days leverage a wide range of techniques and social networking applications to assemble personal and professional data regarding an individual so as to seek out the weakest link in the organization. It is a human-based attack including Impersonation, Shoulder Surfing which is spying on the user, and Reverse Social Engineering; however it also has technological aspects such as Email Attachment, Trojan horse, Botnet, Online Scams, Vishing and Pop up Applications.

In the context of information security, social engineering attack is an act of manipulating individuals psychologically so as to obtain private information, access or get the people to do acts or to reveal confidential information. It tends to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions. While referring to such acts, the euphemism "social engineering" is used.

Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.

Generally objectives of social engineering attackers are to sabotage the individuals by collecting personal information and cause inconvenience and obtaining valuables like confidential data, access, or monitory benefits.

Using this process of social engineering, people can be hacked (manipulated) and their personal information can be obtained and used for fraudulent activities.

Social Engineering attacks have been made against the Twitter accounts of major companies and high profile users such as Barack Obama, U.S. President Joe Biden, Elon Musk, Bill Gates, Kanye West, Michael Bloomberg, and Apple recently in the year 2020. Twitter had to give special protections to the former U.S President Donald Trump’s Twitter account to prevent risk of cyber attack. It is high time to discuss and understand the seriousness of social engineering attacks and ways to prevent the attacks and minimise the chances of being a victim.

Most Famous Social Engineering Attacks:

1. 2020 Twitter Bitcoin Scam:

Twitter Bitcoin scam serves as proof that not even the social media giants are immune to cyber attacks.

Well known Twitter users with the blue verification checkmark Tweeted "double your Bitcoin" offers, informing their followers that they would double the donations made on a select link. Prominent leaders, celebrities, and big brands like former U.S. President Barack Obama, media billionaire Mike Bloomberg, tech creators Apple, and more were among the Twitter accounts affected. The reason being the affected accounts had millions of followers, the attackers could get hundreds of contributions within mere minutes — reportedly totaling over One hundred-thousand US dollars in Bitcoin, according to The BBC.

Through a series of highly-targeted social engineering attacks, the cybercriminals attacked these many high-profile users' accounts in one attack. The cybercriminals manipulated Twitter employees to infect them with malware. From there, they made their way through Twitter's internal systems and gained administrative access to a wealth of verified users' passwords.

2. 2016 US Presidential Election Email Leak

The Democratic campaign's email leak is one of the noteworthy hacks of the last decade.

A series of spear phishing emails were sent by cybercriminals from Russia to various individuals in The Democratic National Convention's network, making it to appear as Google warning recipients of suspicious activity on their Google accounts. The social engineering email shortened the link using a Bitly URL and the true redirect path was hidden.

Once the shortened link was clicked, the webpage directed the recipients to change their password. After targets clicked the spoofed link and entered their credentials, the cyber criminals gained complete access to their Google account including their Gmail access, which allowed them to scrub thousands of emails with sensitive information pertaining to the Democratic candidate Hilary Clinton's campaign.

3. 2013 Yahoo Customer Account Breach

A few years back, Yahoo had every single customer account compromised in a social engineering attack. A significant three billion users had their Yahoo's credentials exposed, some of which were sold on the dark web with the intention of launching further attacks on individuals compromised. Because of this large extent of exposure of the data, this is considered to be one of the worst cyber attacks of the 2000s.

The attack was the result of errors committed by professionals such as high-privilege engineers, who clicked the phishing email.

Another interesting fact is that Yahoo underestimated the number of accounts breached, reporting only 500 million affected which in turn worsened the attack. Only after 4 years, Yahoo revealed the actual extent of the breach which is literally every single user who had an account with Yahoo at the time of the attack. And it was too late to protect the data of affected users.

Social Engineering Attacks in India:

- According to a news article published in The Hindu Business Line on 6th March 2021, the number of internet users increased multi-fold due to pandemic situation that demanded for work from home, meetings in video conference, online shopping and e-learning which resulted in the steady increase in cyber crimes and cyber security breaches, Kaspersky, a Russian multinational cyber security and anti-virus provider said in this regard. It detected and blocked 133,318,878 internet- borne threats in 2020. This affected 35 per cent of the internet users in India, placing India on 43rd rank of worst affected countries globally.

  The share of attacks hosted by servers in India was 0.19 per cent. 7,714,258 incidents in the period January-December 2020 were recorded, placing India in 18th place worldwide.

The attacks were social engineering attacks wherein a user was made to download a malicious file to his/ her device by tricking them into thinking that it was a legitimate program in the guise of various scams related to Covid-19 and other trending issues throughout the year.

Employees and students were cleverly targeted by cybercriminals due to the lack of necessary security solutions on their devices," it said.

- According to a new article in Financial Express published on 29th July 2020, Organisations in India lost Rs 14 Cr on average to data breaches in August 2019 - April 2020 says IBM.

India is witnessing a change in the nature of cyber-crimes, it is now extremely organized and collaborative with rising incidents of phishing attacks, social engineering attacks, etc," Out of the total breach, malicious attacks accounted for 53 per cent as per the findings, system glitches accounted for 26 per cent and the remaining 21 per cent of breaches due to human error.

How to over come these frauds and this crises. Since March 2020 the entire world rest on online business through online applications. India is pushed to Digital India due to pandemic since March 2020. Even courts are functioning through online. The government should be therefore come out with a clear policy and frame laws on these problems of Social Engineering. The CYSI should conduct debates on this issue and give recommendations on this subject. Government should bring in laws to handle and curb the menace of Social Engineering.

Let us now join to transform our unity of interest into a unity of purpose

Hope this webinar will throw much light on the challenges we are now facing and how to deal with this.

I leave way to the Main speaker of today's topic and I thank the organizers once again for giving me this opportunity

Thank you.

.