राष्ट्रीय इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी संस्थान, रोपड़

National Institute of Electronics and Information Technology (NIELIT), Ropar

SOCIAL NETWORKING
&
SOCIAL ENGINEERING

SHRI AKASH SHARAN

SCIENTIST 'B', NIELIT

CONTENT OF THE PRESENTATION

- Digital Era
- Social Networking
- Evolution of Social Networking
- Use of Social Networking
- Benefits of Social Networking
- Negative Impact of Social Networking
- Cyber Security Concerns
  - Cyber Threat
  - Social Engineering
  - Social Engineering Life Cycle
  - Phishing
  - India’s Scenario
  - Phishing Process
  - Drive by Download
  - Mal-Advertisement

The world that we live in !

Digital Era

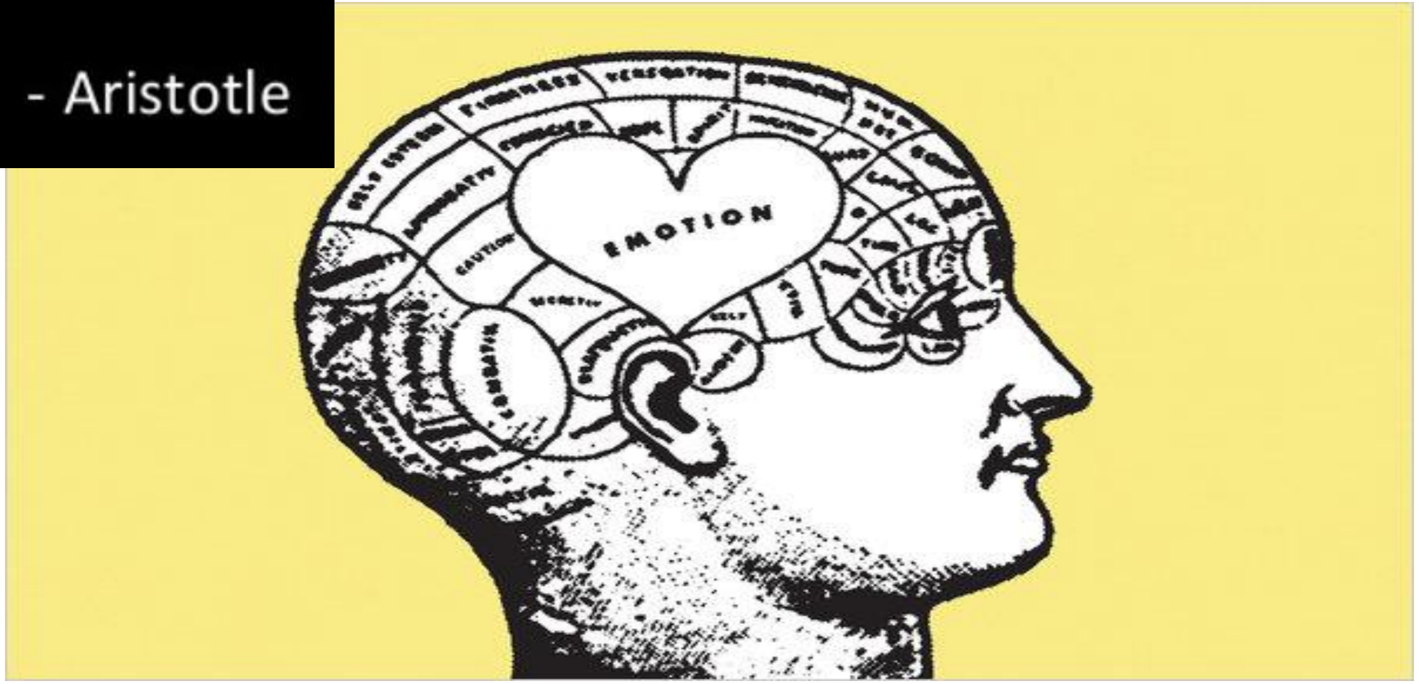
Internet Uses Stats

- According to the 2019 report by the **Internet & Mobile Association of India (IAMAI) and Nielsen -** With over 503 million internet users, India is the second largest online market in the world, ranked only behind China. It was estimated that by 2023, there would be over 650 million internet users in the country that have been already crossed.
- 227 million active internet user in rurals, 10% more than urban India's about 205 million as per same report.
- **71 Million kids between 5-11 age also go online using adult device.**
- Overall gender distribution -: Men : 65% & Women : 35%

Social Networking

Connecting People in the Digital Era

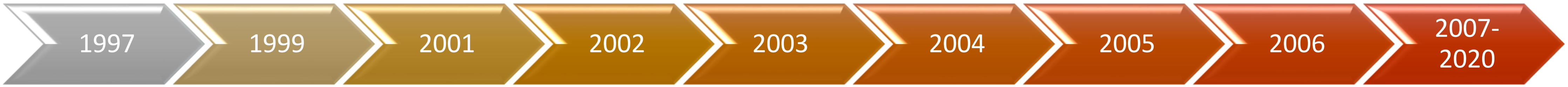
> "Man is by nature a social animal…anyone who either cannot lead the common life or is so self-sufficient as not to need to, is either a beast or a god."
>
> \- Aristotle



Social Networking

- A Social networking service is an online platform which people use to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections.
- Social media platforms are enjoyable to use, beneficial while looking for a job, and excellent for staying in touch with friends, family, and business associates.
- Social networks have billions of users worldwide, making them an integral part of modern society.

Evolution of Social Media



1997
- Short-lived Six Degrees profile uploading service

1999
- Webblogs or blogs

2001
- Friendster : Email registration and basic online networking

2002
- Linkedin

2003
- Myspace

2004
- Facebook

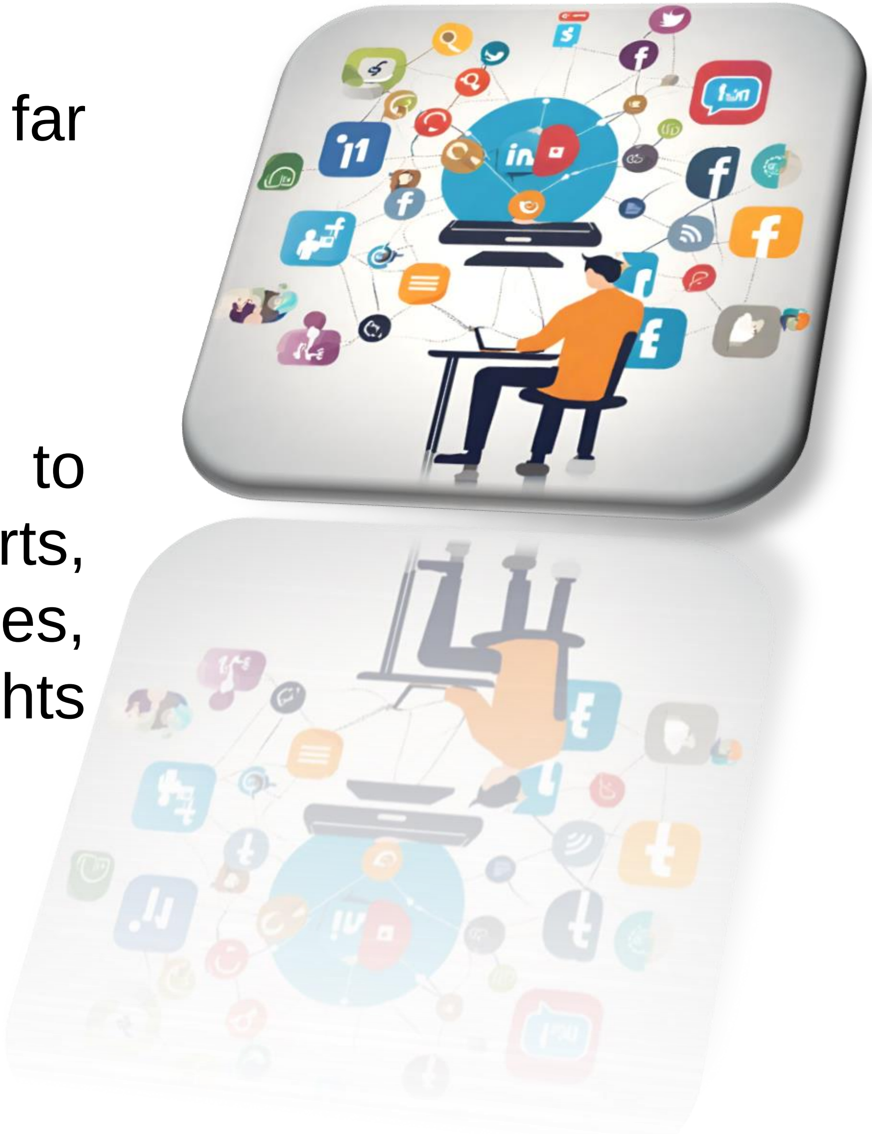
2005
- Reddit
- Youtube

2006
- Twitter

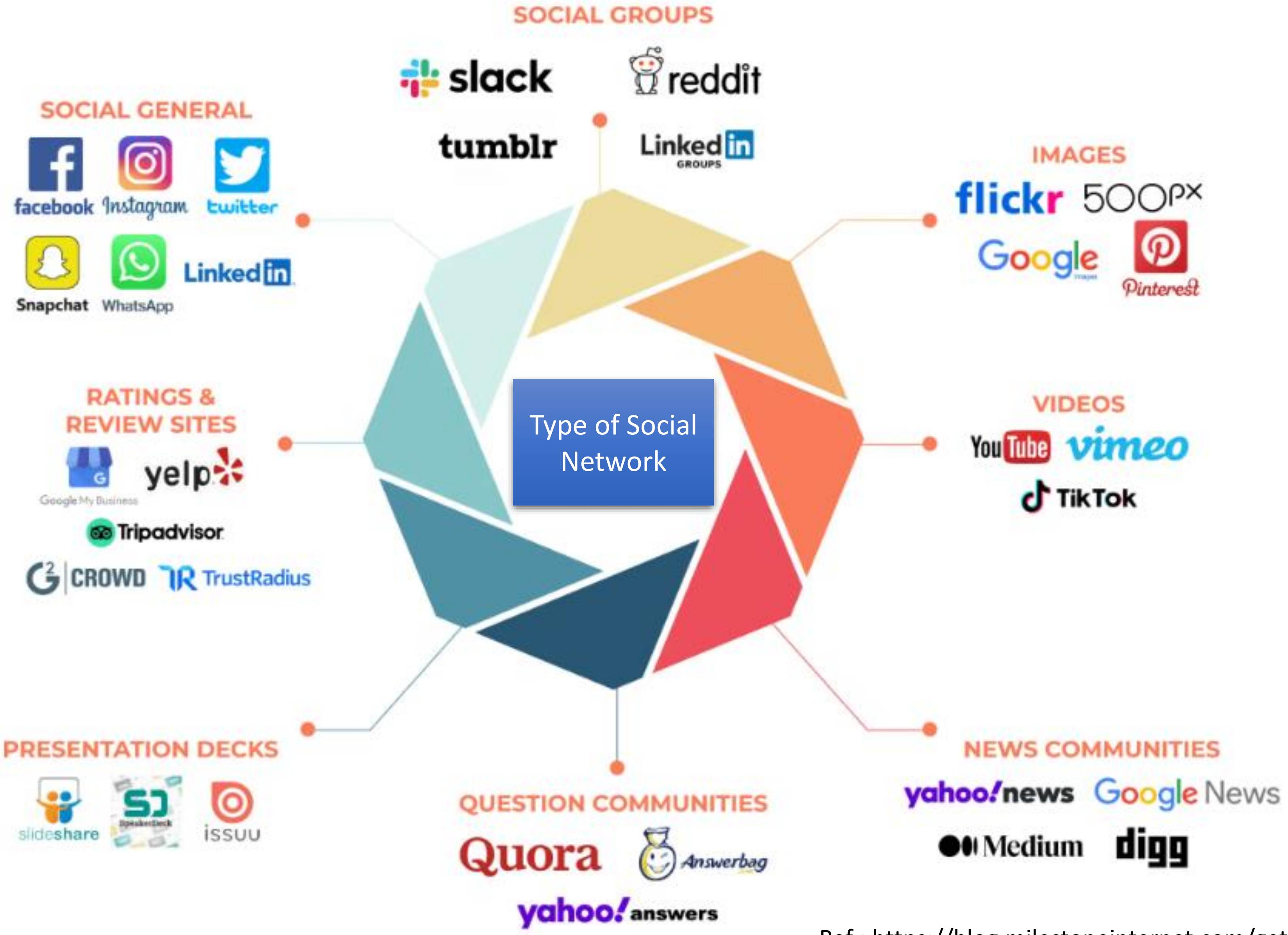
2007-2020
- Instagram
- Tiktok
- Snapchat etc

Use of Social Networking

- Meeting the people online across the world.
- Making friendship with the people who are far away.
- Profile building.
- Self representation.
- Exchanging / Sharing the information related to studies or education, current affairs, sports, business, transport, movies, latest news updates, event announcements, exchanging the thoughts etc.
- Share the data files, videos, music, photo e.t.c

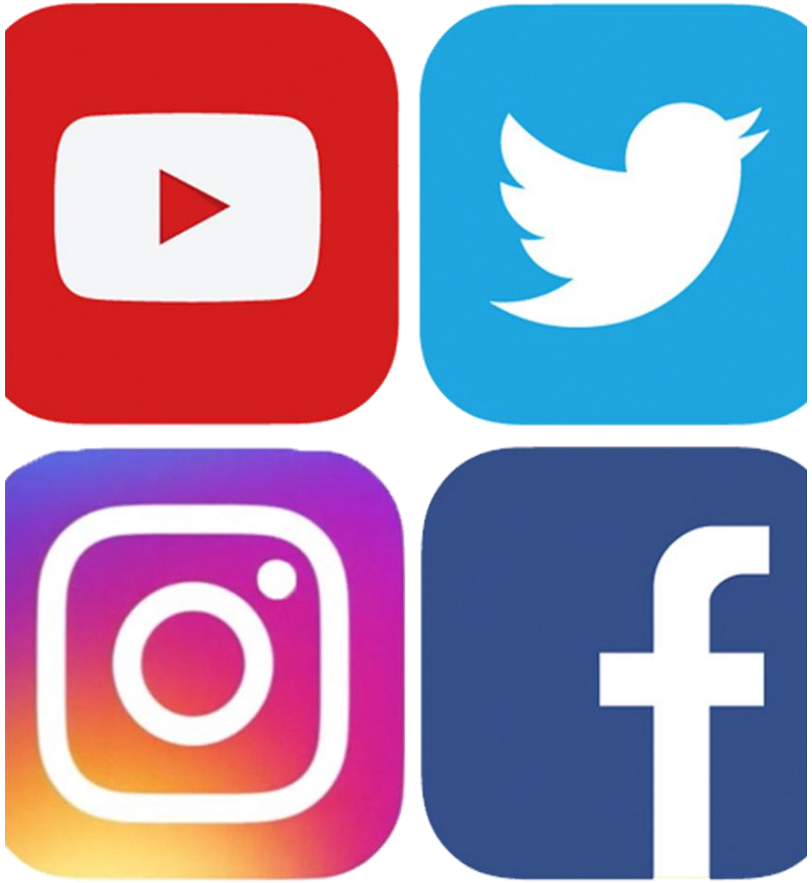


Types of Social Networking



Ref : https://blog.milestoneinternet.com/getting-social/social-media-starfish/

Future Trends in Social Media



- Video content will continue to dominate social media platforms.
- Social commerce will become more prominent, allowing users to make purchases directly within social media apps.
- Augmented Reality (AR) will be integrated into social media platforms, providing interactive and immersive experiences.

Benefits of Social Networking

Improved Communication

- Social networks allow people to connect and communicate instantly.

Networking opportunities

- Social networks help individuals expand personal and professional connections.

Information Sharing

- Users can easily share news, articles, and other valuable resources.

Global reach

- Social networks enable interactions with people from different countries and cultures.

Strengthened connections

- Social networks help maintain and strengthen friendships and family ties.

Support communities

- Social networks offer support groups for various interests and issues.

Excessive use of social networks can negatively impact real-life relationships.

Negative Impacts

Physical Health

- Chest pain, back pain, and headaches.
- Sleep-related issues
- Less Exercise
- Obesity
- Eyestrain
- Affecting Posture

Emotional Health

- Addiction
- Sadness
- Stress
- Increased risk of depression, anxiety, loneliness, self-harm, and suicidal thoughts.

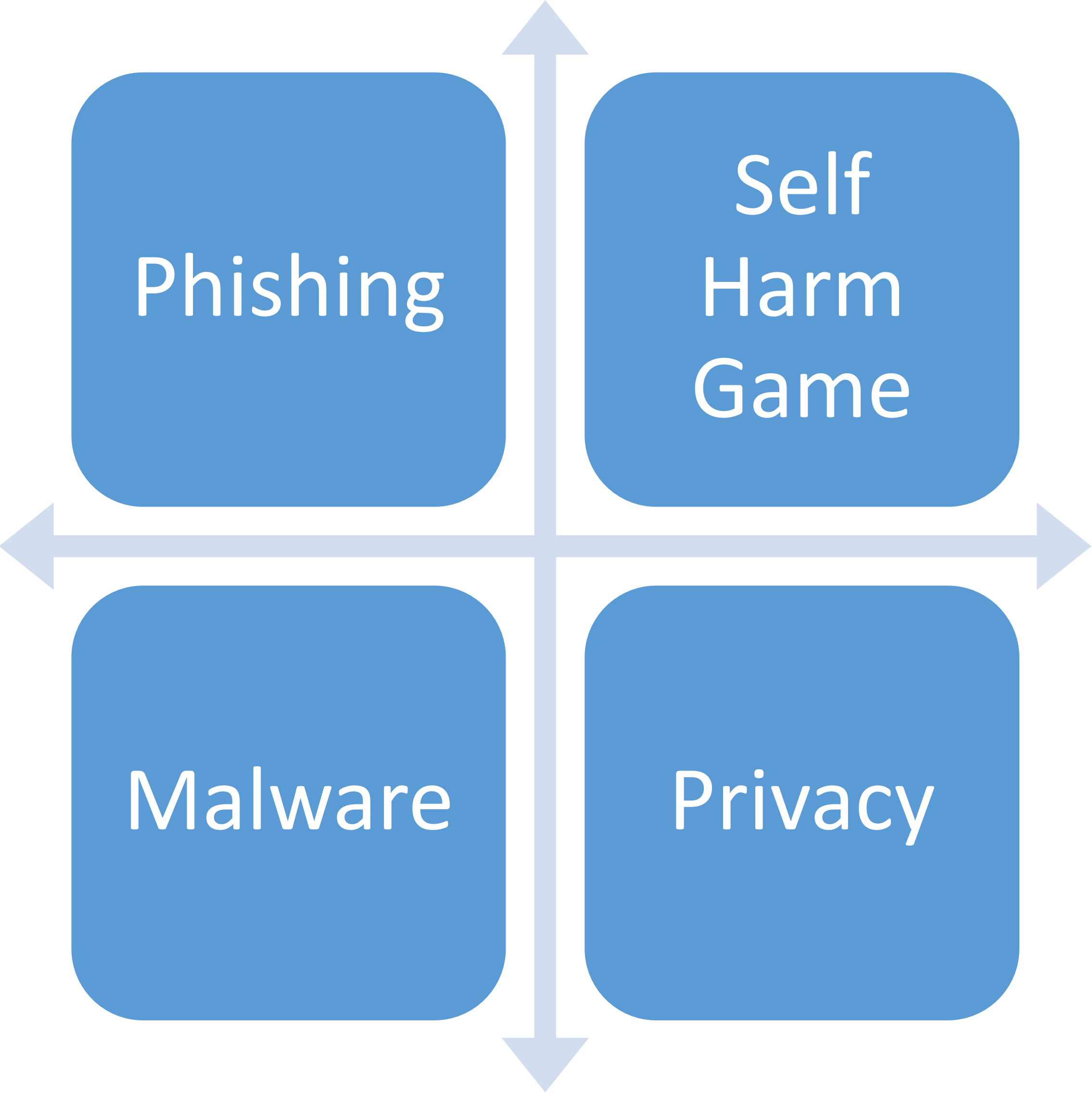
Psychological Health

- “Phubbing,” which refers to the extent to which an individual uses, or is distracted by, their smartphone during face-to-face.
- Pressure to compare oneself to others

Interpersonal Relationships

- People who rely too much on social media for communication may overlook in-person encounters, which are crucial for the growth and maintenance of social skills.
- Social media can encourage the dissemination of false information and fake news which can weaken social ties and cause trust to break down.

Cyber Security Concerns

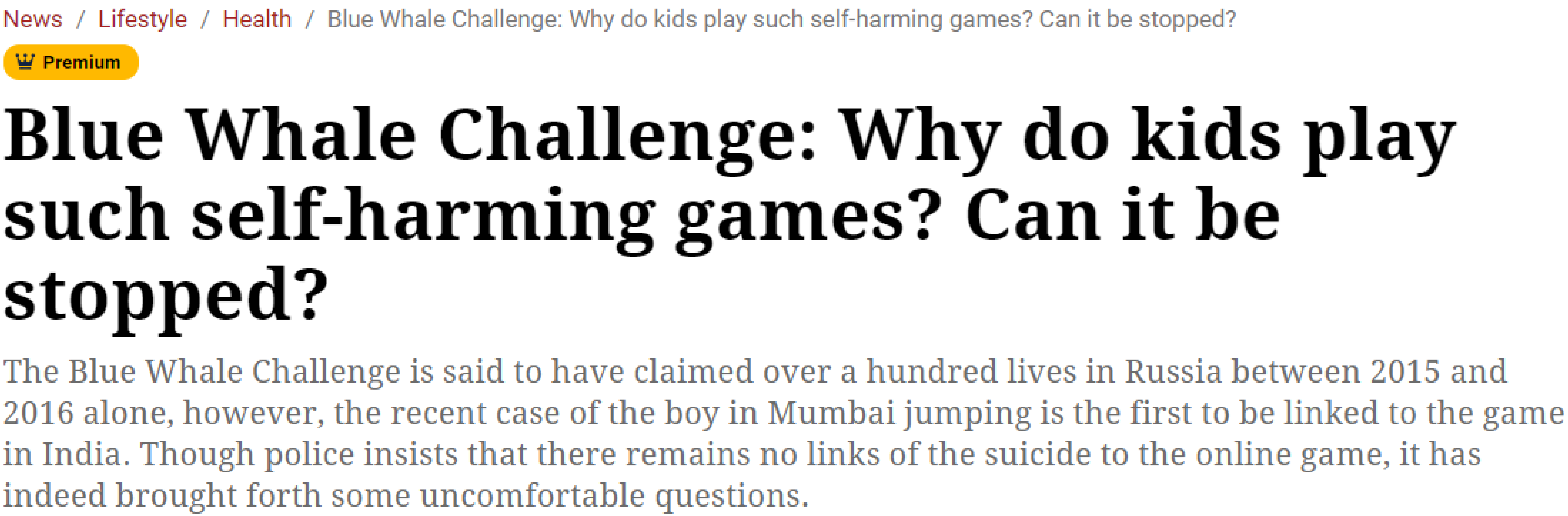


Phishing

Self Harm Game

Malware

Privacy

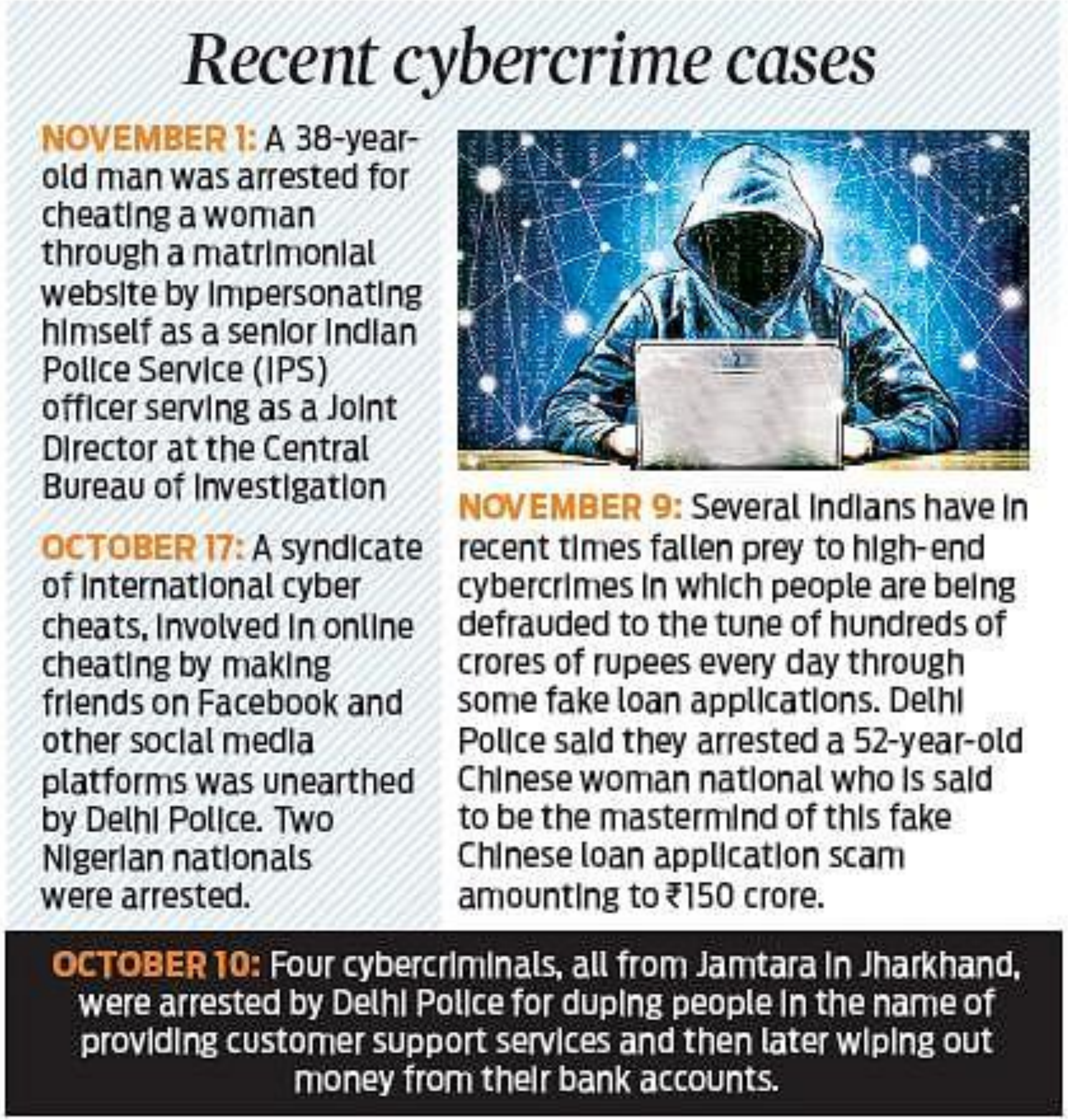


News / Lifestyle / Health / Blue Whale Challenge: Why do kids play such self-harming games? Can it be stopped?

Premium

Blue Whale Challenge: Why do kids play such self-harming games? Can it be stopped?

The Blue Whale Challenge is said to have claimed over a hundred lives in Russia between 2015 and 2016 alone, however, the recent case of the boy in Mumbai jumping is the first to be linked to the game in India. Though police insists that there remains no links of the suicide to the online game, it has indeed brought forth some uncomfortable questions.



Recent cybercrime cases

NOVEMBER 1: A 38-year-old man was arrested for cheating a woman through a matrimonial website by impersonating himself as a senior Indian Police Service (IPS) officer serving as a Joint Director at the Central Bureau of Investigation

OCTOBER 17: A syndicate of international cyber cheats, involved in online cheating by making friends on Facebook and other social media platforms was unearthed by Delhi Police. Two Nigerian nationals were arrested.

NOVEMBER 9: Several Indians have in recent times fallen prey to high-end cybercrimes in which people are being defrauded to the tune of hundreds of crores of rupees every day through some fake loan applications. Delhi Police said they arrested a 52-year-old Chinese woman national who is said to be the mastermind of this fake Chinese loan application scam amounting to ₹150 crore.

OCTOBER 10: Four cybercriminals, all from Jamtara in Jharkhand, were arrested by Delhi Police for duping people in the name of providing customer support services and then later wiping out money from their bank accounts.

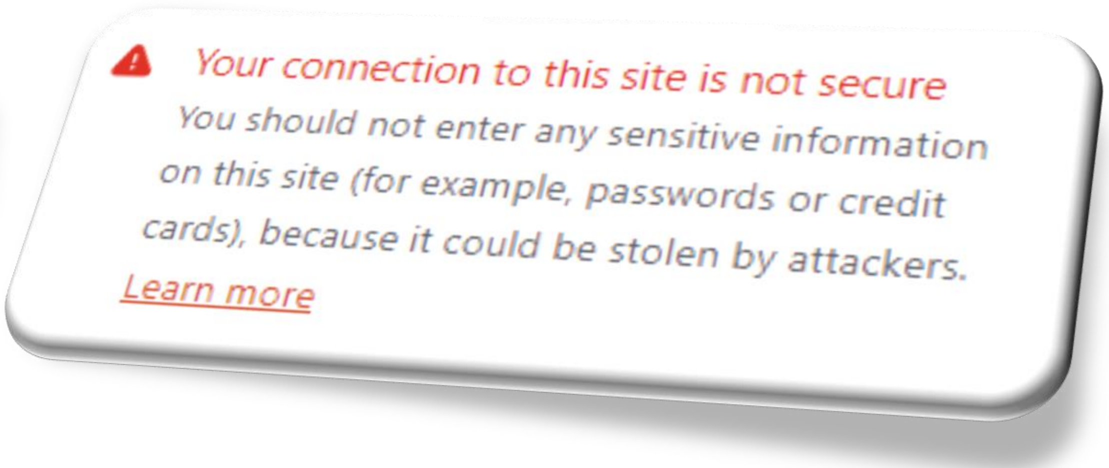
Ref: https://www.newindianexpress.com/

Social Engineering :The Art of Deception

Understanding the Tactics and Strategies of Social Engineering

Cyber Threat

Cyber threat is any circumstance or event with the potential to adversely impact Organisation (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.

Who are these people

- Hackers : Black, white , grey !
- Curious Kids or enthusiasts
- Professional Criminals – Group of experienced hackers
- Malware programmers
- Corporate Espionage
- Information warfare
- Cyber Terrorism
- State Players
- Stake holders – Employees, Vendors?

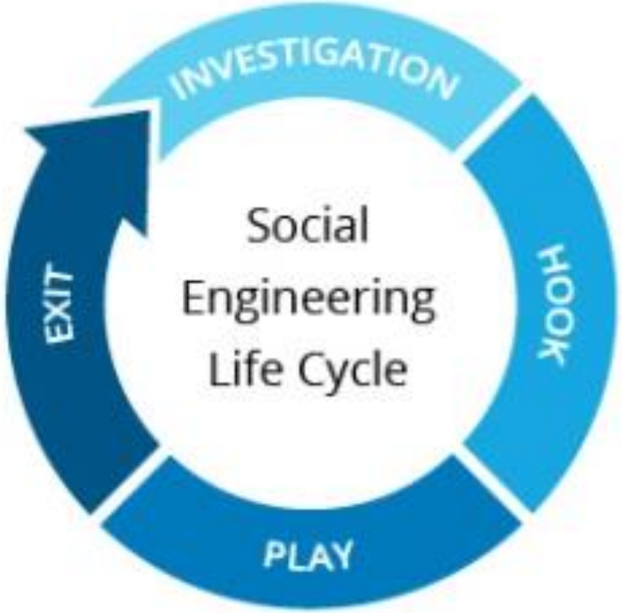
Social Engineering Attack

- Social engineering is the term used for a broad range of malicious activities accomplished through human interactions.
- It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack.
- Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Social Engineering Lifecycle

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).



Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Phishing

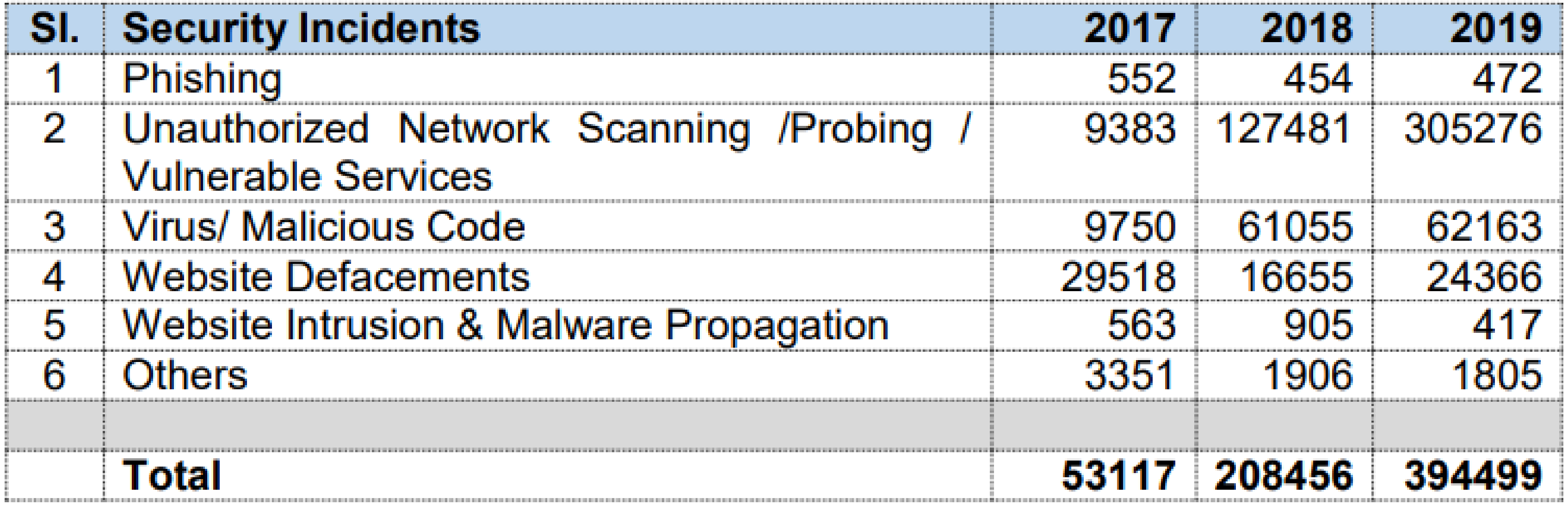
Most of the attacks on financial institutions the past 3 years have NOT been through brute force attacks on firewall appliances, it has been through acquiring users' passwords, this technique is called "Phishing"

Phishing Types

- **Phishing:** Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
- **Spear phishing:** Phishing attempts directed at specific individuals or companies have been termed spear phishing.
- **Whaling:** The term whaling has been coined for spear phishing attacks directed specifically at senior executives and other high-profile targets.
- **Vishing:** The term is a combination of 'voice' and 'phishing'.

Indian Scenario

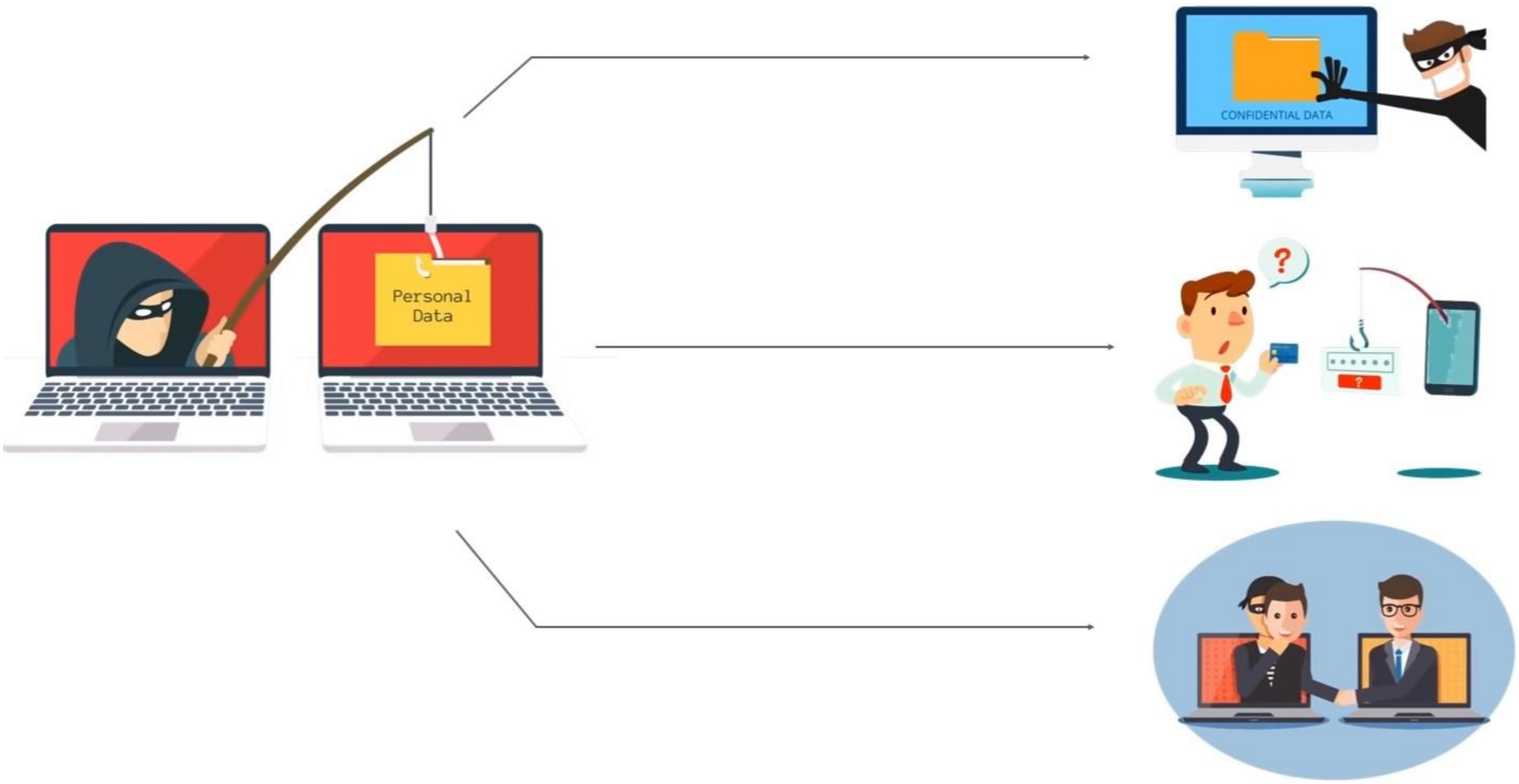
- CERT-IN is a functional organisation of Ministry of Electronic and Information Technology, Government of India. CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community.



Sl.	Security Incidents	2017	2018	2019
1	Phishing	552	454	472
2	Unauthorized Network Scanning /Probing / Vulnerable Services	9383	127481	305276
3	Virus/ Malicious Code	9750	61055	62163
4	Website Defacements	29518	16655	24366
5	Website Intrusion & Malware Propagation	563	905	417
6	Others	3351	1906	1805
	Total	**53117**	**208456**	**394499**

- The Financial Stability Report, July 2020 published by the Reserve Bank, states that the banking industry is a target of choice for Cyber-attacks. It further observes that there has been an increased incidence of cyber threats in the post COVID-19 lockdown period.

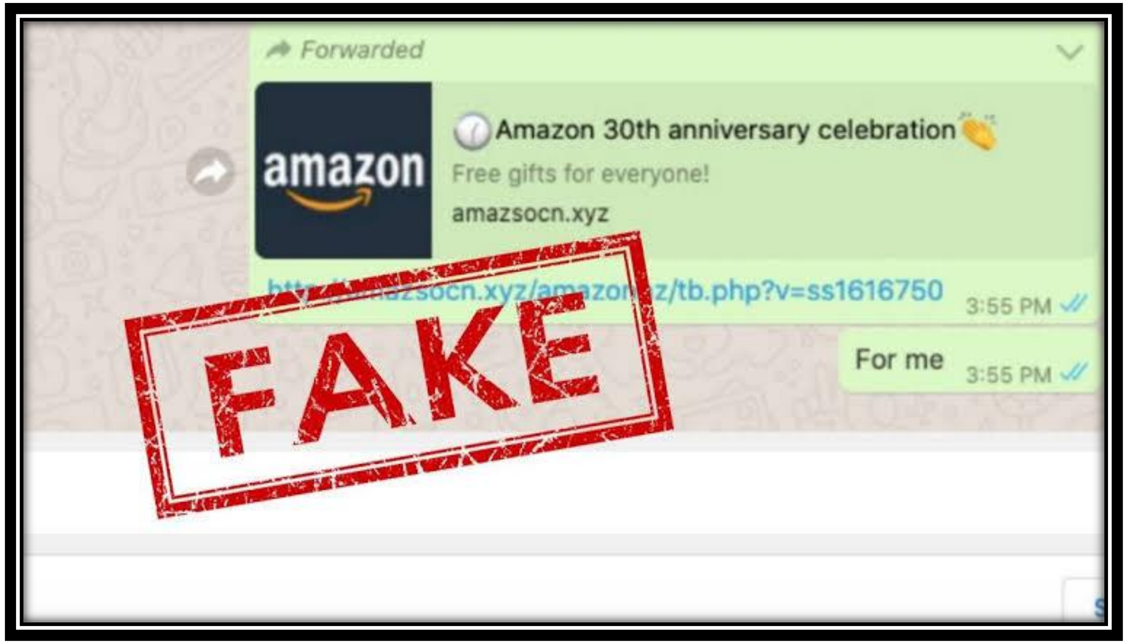
Phishing Process



Stealing Confidential Data

Harvesting Login Credential

Impersonating



Forwarded

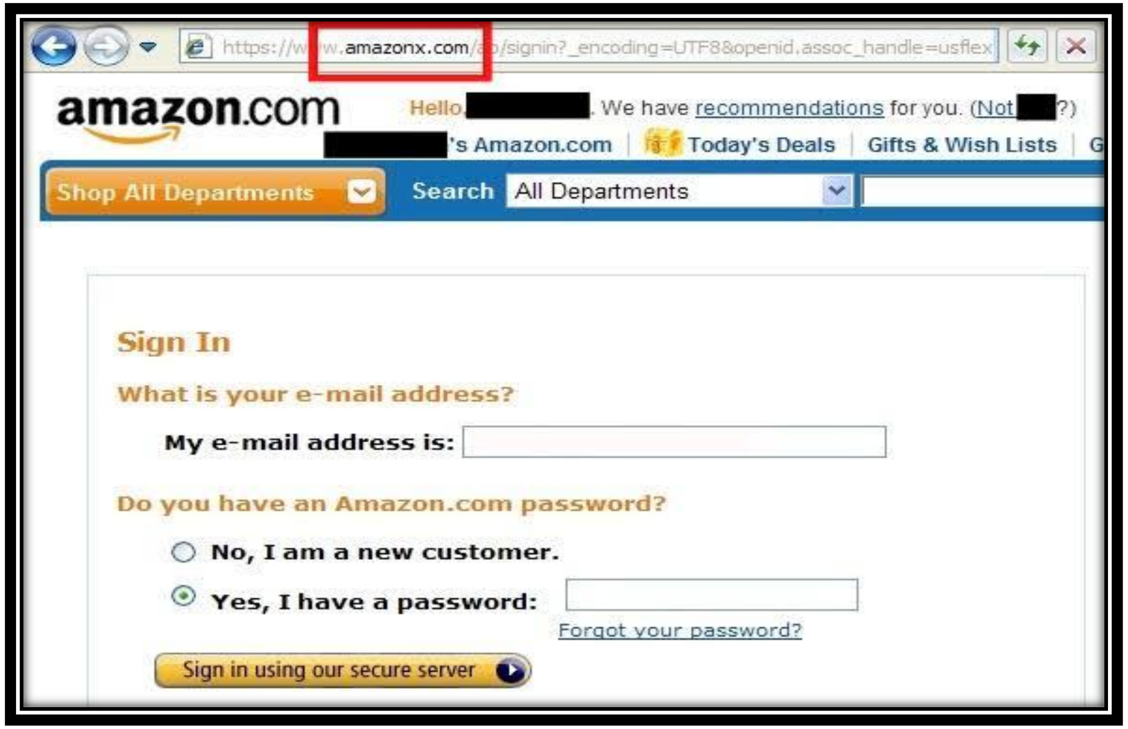
Amazon 30th anniversary celebration 👏

Free gifts for everyone!

amazsocn.xyz

http://amazsocn.xyz/amazonbz/tb.php?v=ss1616750 3:55 PM

For me 3:55 PM



https://www.amazonx.com/ap/signin?_encoding=UTF8&openid.assoc_handle=usflex

Hello, [redacted]. We have recommendations for you. (Not [redacted]?)

[redacted]'s Amazon.com | Today's Deals | Gifts & Wish Lists | G

Sign In

What is your e-mail address?

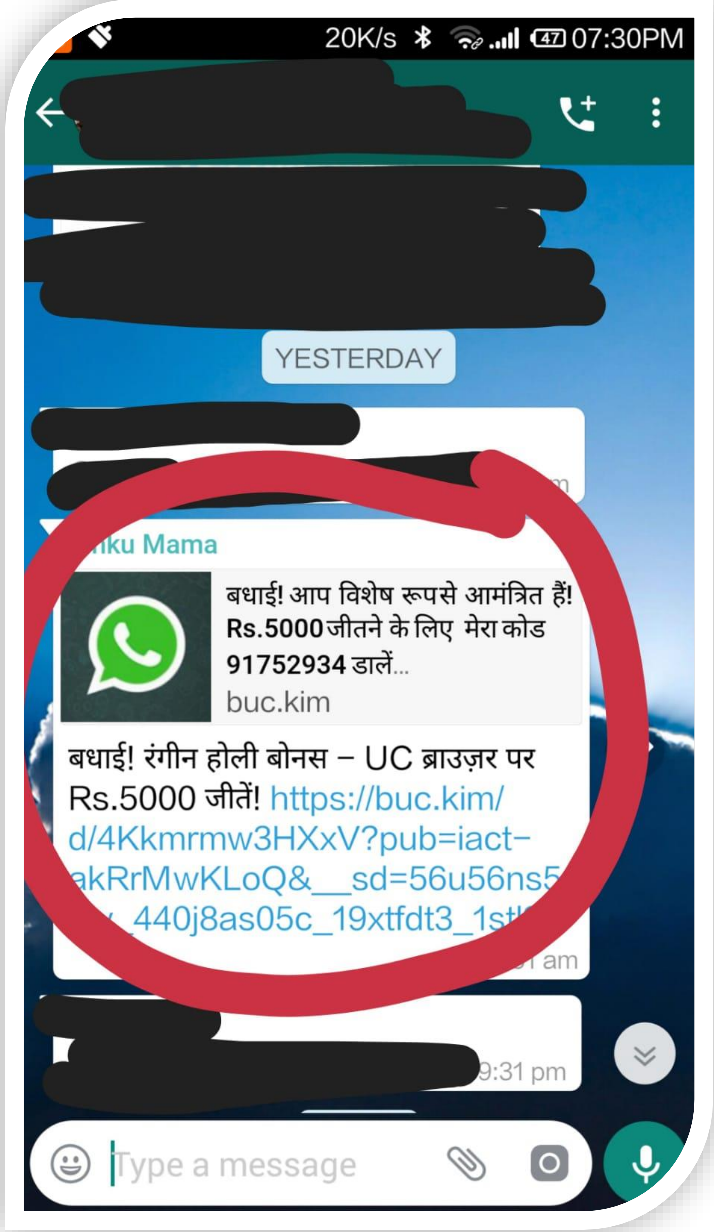
My e-mail address is:

Do you have an Amazon.com password?

○ No, I am a new customer.

● Yes, I have a password:

Forgot your password?



20K/s 47 07:30PM

[redacted]

[redacted]

YESTERDAY

[redacted]

...ku Mama

बधाई! आप विशेष रूपसे आमंत्रित हैं! Rs.5000 जीतने के लिए मेरा कोड 91752934 डालें...

buc.kim

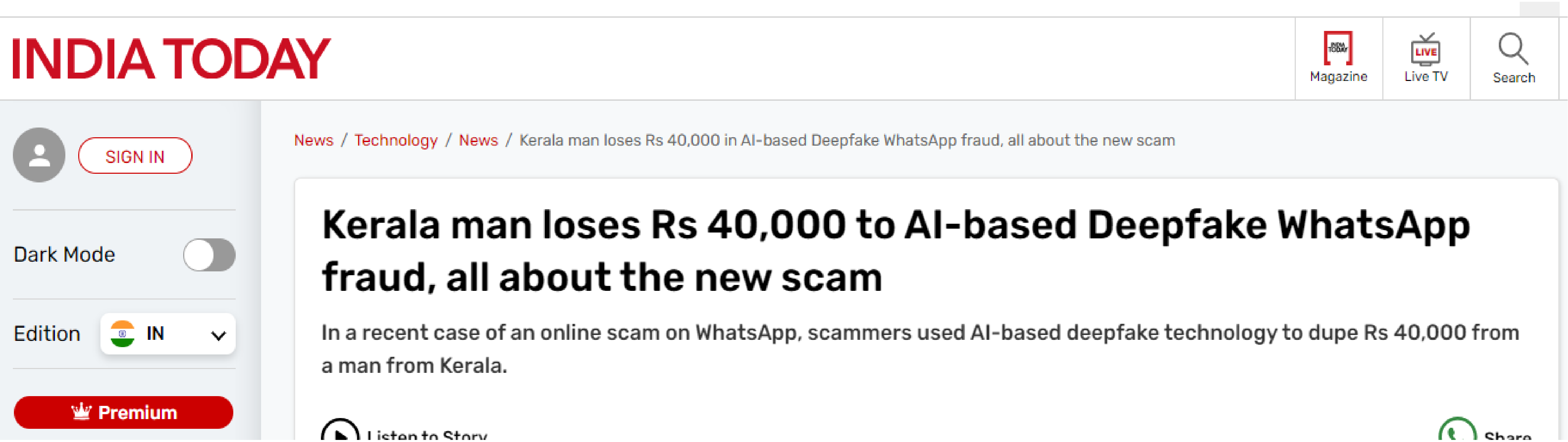
बधाई! रंगीन होली बोनस – UC ब्राउज़र पर Rs.5000 जीतें! https://buc.kim/d/4Kkmrmw3HXxV?pub=iact-akRrMwKLoQ&__sd=56u56ns5 _440j8as05c_19xtfdt3_1st

am

[redacted]

9:31 pm

AI-Based Deep Fake Phishing



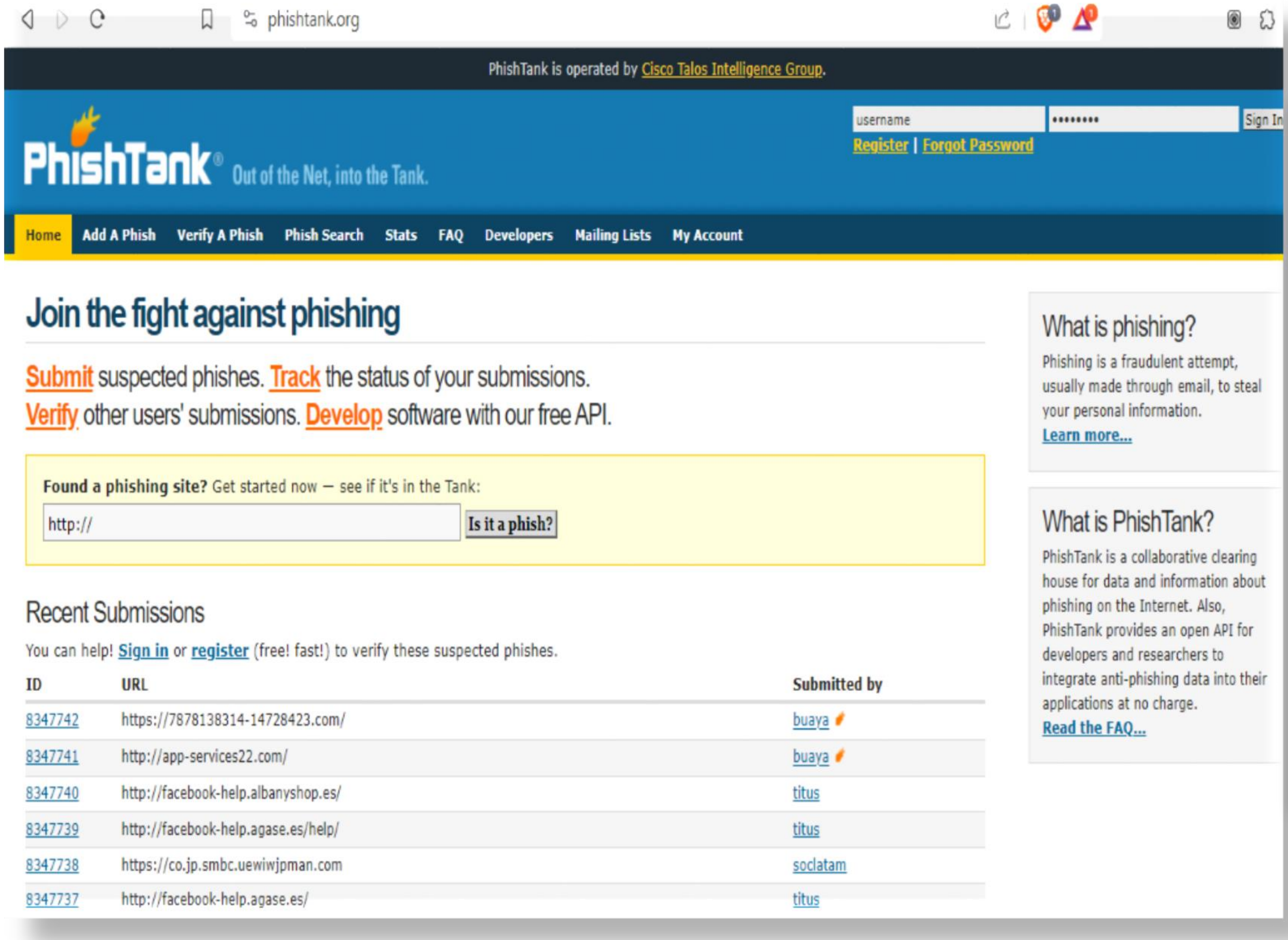
News / Technology / News / Kerala man loses Rs 40,000 in AI-based Deepfake WhatsApp fraud, all about the new scam

Kerala man loses Rs 40,000 to AI-based Deepfake WhatsApp fraud, all about the new scam

In a recent case of an online scam on WhatsApp, scammers used AI-based deepfake technology to dupe Rs 40,000 from a man from Kerala.

Artificial intelligence is used in a particular kind of scam called "AI-based deep fake calls," which produces phony audio or video recordings of real people. These calls can be made by scammers posing as a reliable friend, relative, or acquaintance in an attempt to deceive the victim into divulging personal information or money.

Phishing Reporting and Checker



PhishTank is operated by Cisco Talos Intelligence Group.

PhishTank® Out of the Net, into the Tank.

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
8347742	https://7878138314-14728423.com/	buaya
8347741	http://app-services22.com/	buaya
8347740	http://facebook-help.albanyshop.es/	titus
8347739	http://facebook-help.agase.es/help/	titus
8347738	https://co.jp.smbc.uewiwjpman.com	soclatam
8347737	http://facebook-help.agase.es/	titus

What is phishing?

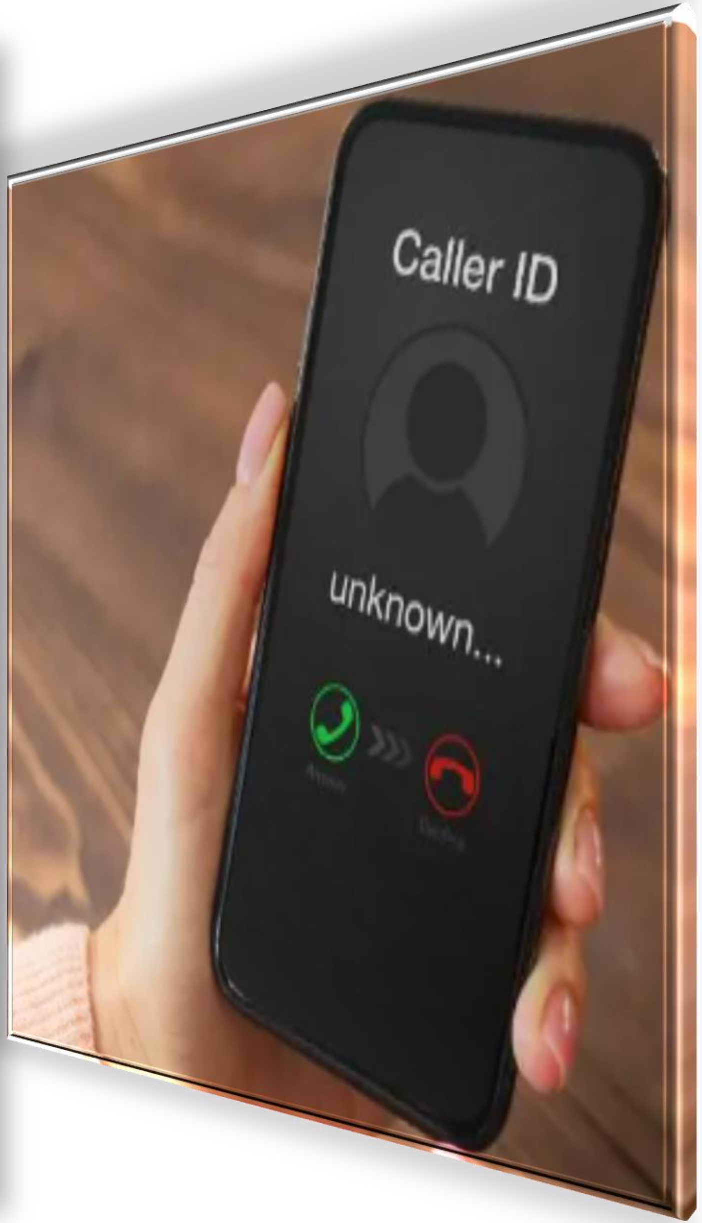
Phishing is a fraudulent attempt, usually made through email, to steal your personal information.

Learn more...

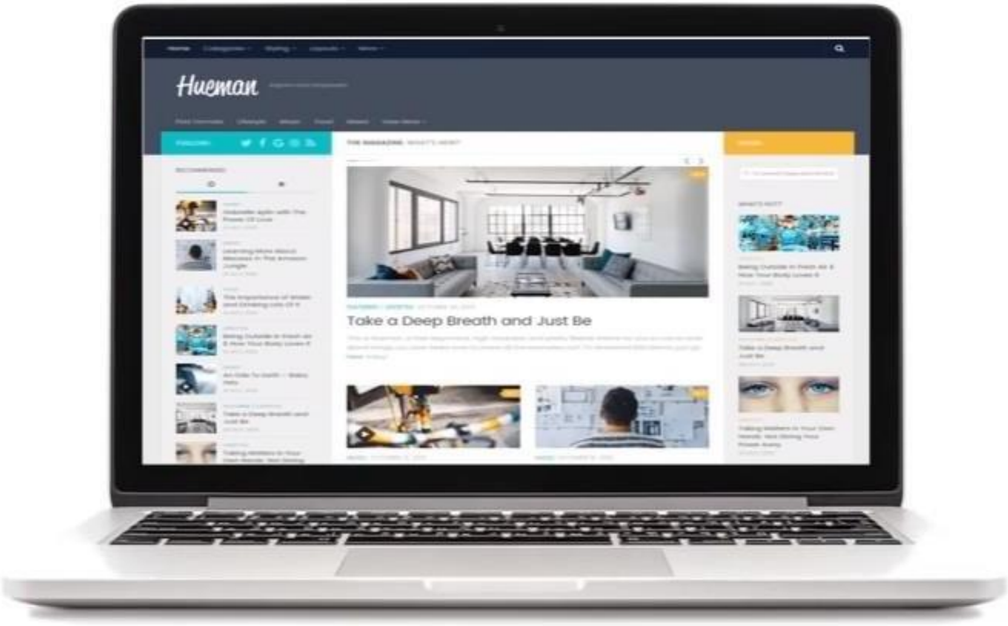
What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.

Read the FAQ...



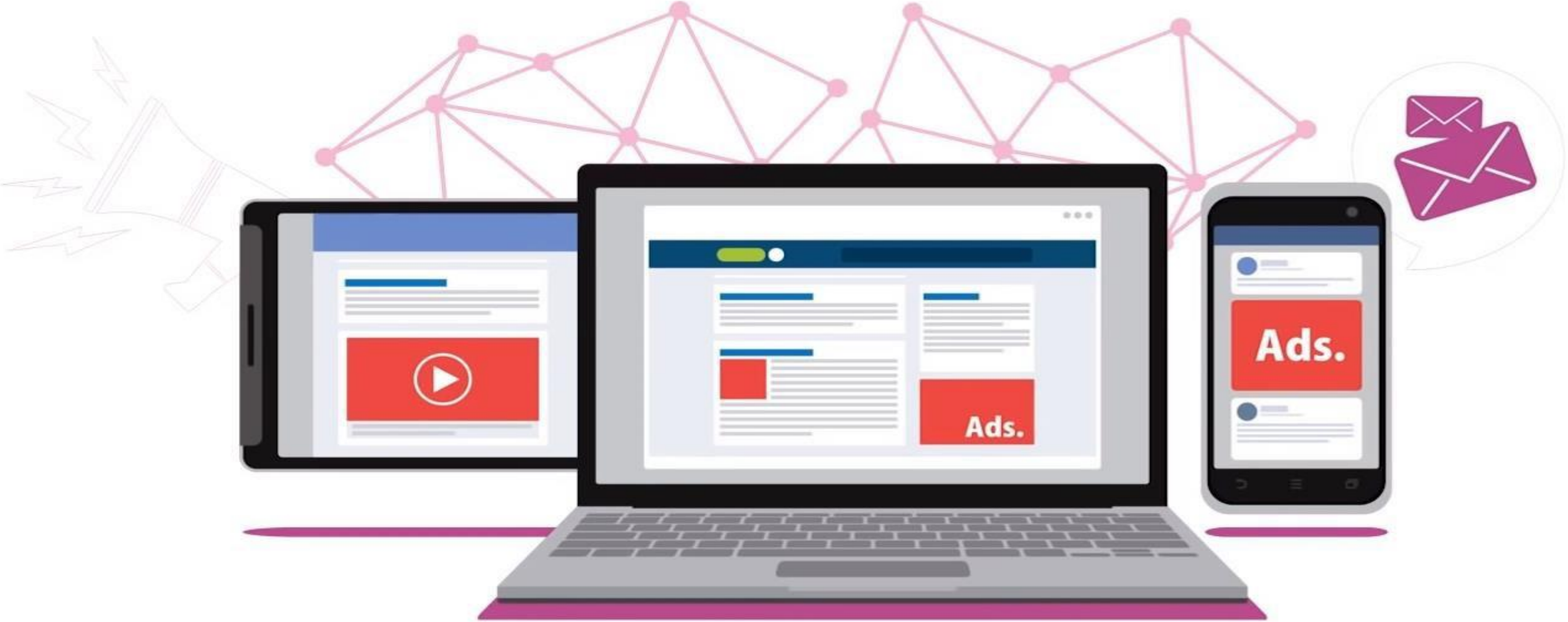
Drive-by Downloads



Drive-by download attacks occur when vulnerable computers get infected by just visiting a website. Findings from latest Microsoft Security Intelligence Report and many of its previous volumes reveal that Drive-by Exploits have become the top web security threat to worry about.

Malvertising

Malvertising is the name we in the security industry give to criminally-controlled adverts which intentionally infect people and businesses. These can be any ad on any site – often ones which you use as part of your everyday Internet usage. It is a growing problem, as is evidenced by a recent US Senate report, and the establishment of bodies like Trust In Ads.



रा.इ.सू.प्रौ.सं NIELIT

आज का साइबर (Cyber) सुविचार

साइबर (Cyber) सेक्यूरिटी (Security) की जागरूकता हर नागरिक के लिए ज़रूरी है, बिन इसके ज्ञान के साइबरस्पेस (Cyberspace) में ज़िंदगी अधूरी है

Thankyou