AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY

19CSE337 Social Networking and Security

Lecture 24

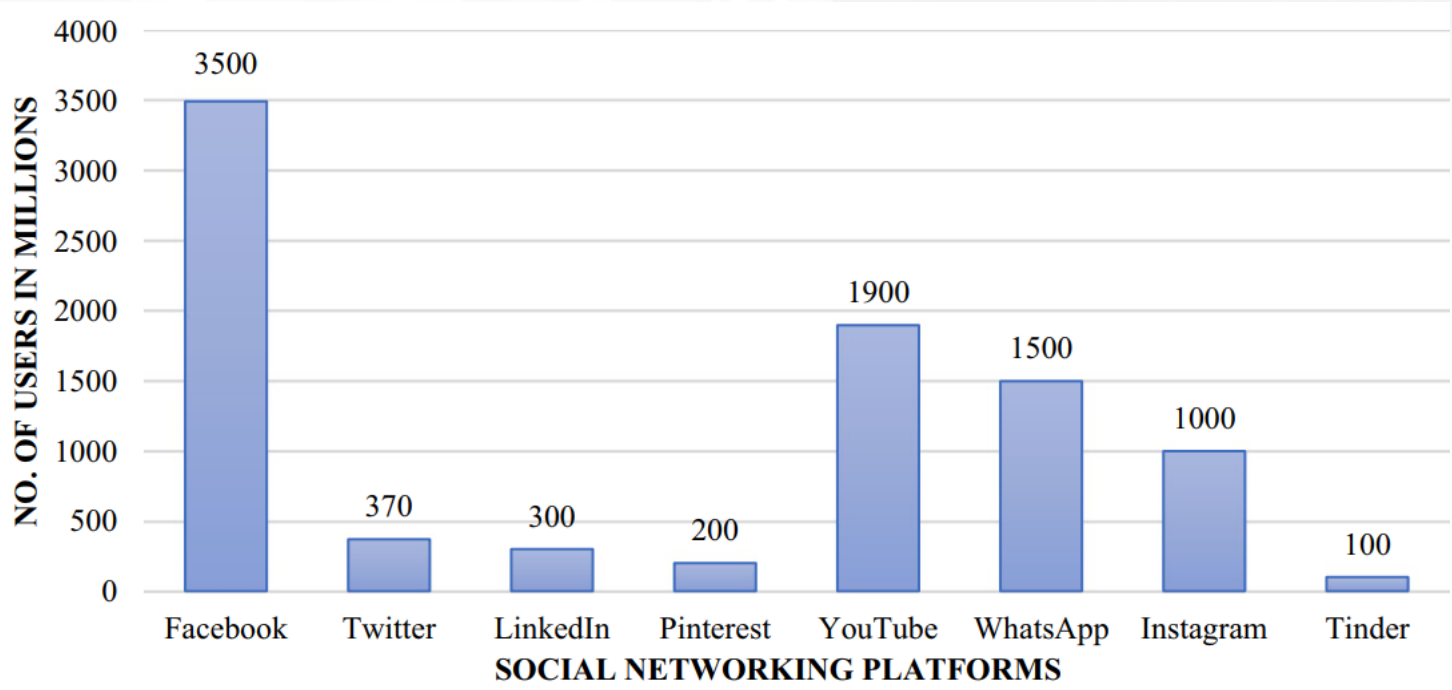
Topics to Discuss

- Security Threats in Social Networking Sites.

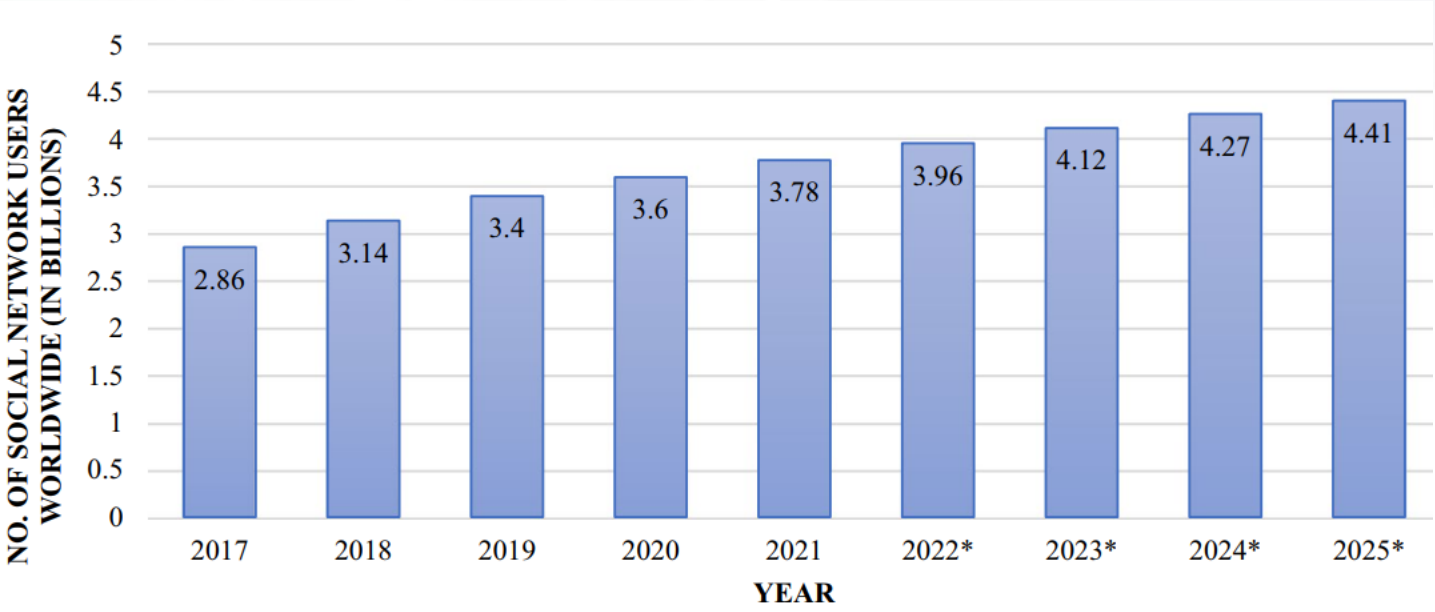
Social Network Security

- A Social Network Service is a kind of web service for establishing a virtual connection between people with similar interests, backgrounds, and activities.
- A SNS allows its users to find new friends, and expand their circle of friends.
- Data sharing is the key feature of a SNS where users are able to share their interests, videos, photos, activities and so on.

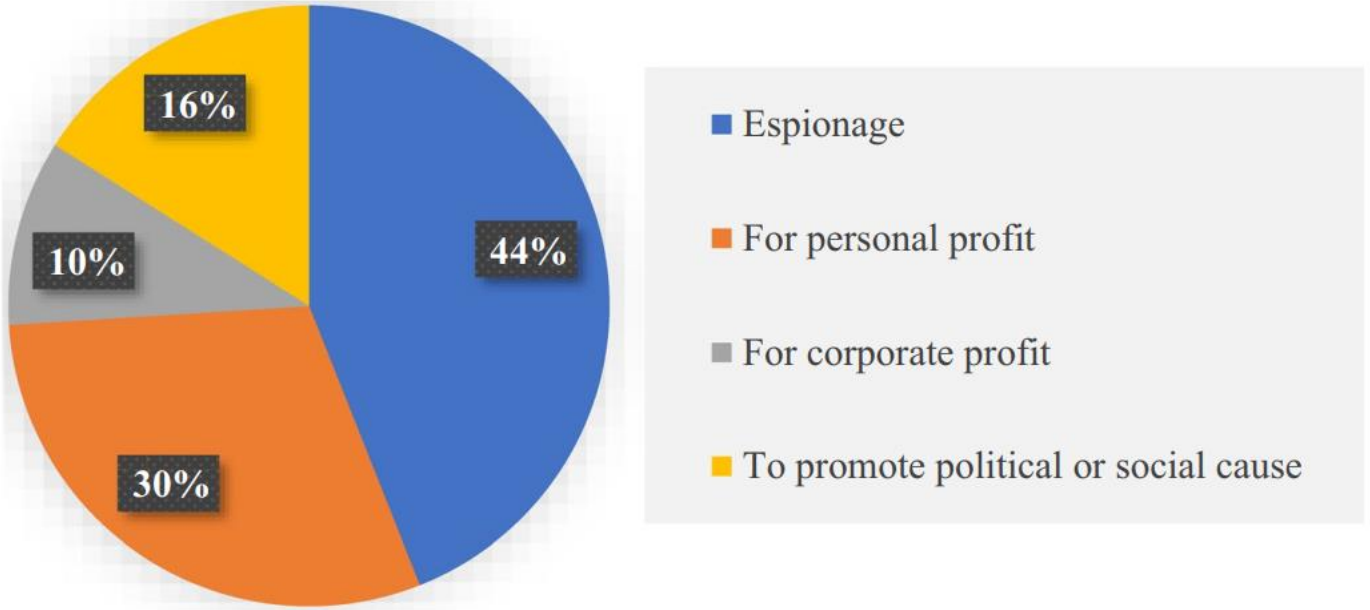
No. of users in different SN platforms



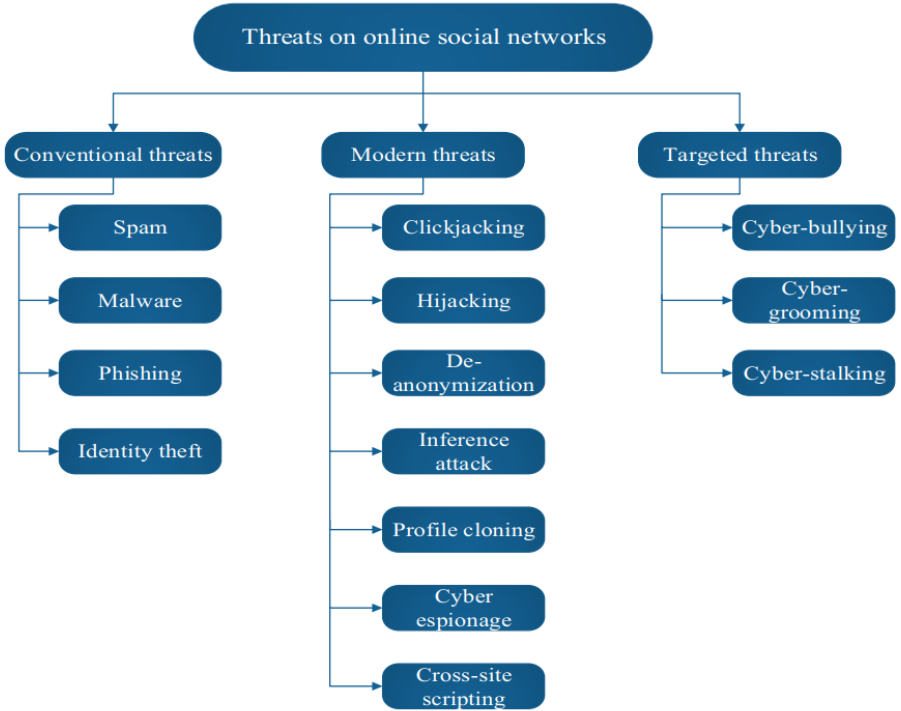
No. of social media users year wise



Most punishable types of hacking in 2021



OSN Threats


Threats on online social networks
Conventional threats
Spam
Malware
Phishing
Identity theft
Modern threats
Clickjacking
Hijacking
De-anonymization
Inference attack
Profile cloning
Cyber espionage
Cross-site scripting
Targeted threats
Cyber-bullying
Cyber-grooming
Cyber-stalking

Spam Attacks

- Unsolicited bulk electronic messages.
- E-mails are conventional way, but OSNs are also successful in spreading spam.
- Most spams are commercial advertisements but they can be used to collect sensitive information from users or may contain viruses, malware or scams.

Malware Attacks

- Malware is a noxious programming which is explicitly evolved to contaminate or access a computer system without the information of the user.
- It may get installed by clicking any URL that will run a script in the system to collect sensitive information.
- In social networking platforms, the malware uses OSNs structure to propagate itself such as the number of vertices, no. of edges, average shortest path and longest path.

Phishing

- A kind of social engineering attack where the aggressor can acquire sensitive and confidential information like user name, password and credit card details of a user through fake websites and emails which appears to be real.
- An invader can impersonate an authentic user to send fake messages to other users via OSN platforms which contains malicious URL.
- This URL will redirect user to a phony website where it asks for personal information.
- In SNS, for example, user gets a message says “Your personal pictures are shared on this website, please check”.

Identity Theft

- Assailant utilizes someone else's identity like social security number, address, mobile number etc.
- With the help of these details, the attacker can easily gain access to a victim's friend list and demand confidential information from them.

Cross Site Scripting Attack

- Also known as XSS or Self-XSS.
- Fundamentally, the attack executes a malicious javascript on the victims browser.
- The browser can be hijacked with just a single click of a button which may send a malicious script to server.
- This script is boomeranged back to the victim and executed on the browser.
- Attractive links and buttons in popular social media sites like twitter and facebook can trick the user into following URLs.

Profile Cloning Attack

- In this attack, the attacker clones the user's profile about which he has a prior knowledge.
- The attacker can use this cloned profile either in the same or different social networking platform to create a trusting relationship with the real user's friends.
- Once connection is established, the attacker tricks the victim's friends to believe in the validity of the fake profile and catch confidential information successfully which is not shared in their public profiles.

Hijacking

- In hijacking, the adversary compromises or takes the control of a user’s account to carry out online frauds.
- The sites without multi-factor authentication and accounts with weak passwords are more vulnerable to hijacking.

Inference Attack

- Inference attack infers a person's confidential information which the user may not want to disclose through other statistics that is put out by the user on some social networking sites.
- It uses data mining procedures on visibly available data like user's friend list, and network topology.
- Using this technique, an attacker can find an organisation's secret information or a user's geographical and educational information.

Sybil Attack

- In Sybil attack, a node claims multiple identities in a network.
- It can be harmful to social networking platforms as they contain a huge number of users who are coupled through a peer to peer network.
- P-2-P can share records straightforwardly without the need of a central server.
- One online entity can make several fake identities to distribute junk information, malware or even affect the reputation and popularity of an organisation.
- For example, a web survey voting where an aggressor can outvote a genuine candidate.

Clickjacking

- Clickjacking is a procedure in which the invader deceives a user to click on a page that is different from what he intended to click.
- It is also known as user interface redress attack.
- Browser vulnerability is used to execute this attack.
- Here, the attacker loads a transparent layer of another page over one the user want to access.

De-Anonymization Attack

- In some SNS like Twitter, and Facebook users can hide their real identity.
- The attackers will try to uncover their identity via tracking cookies, user group enrolment, network topology, browsing history etc.
- It is a kind of information mining.

Cyber Espionage

- Cyber espionage is an act that uses cyber capabilities to gather sensitive information.
- These attacks are motivated by greed for monetary benefits.
- Attackers will collect email address, SNS activities, connections etc.

Cyber bullying

- Harassing a user through emails, phone conversations, chats, publishing pictures etc.
- Continuous process mostly through social networking sites.

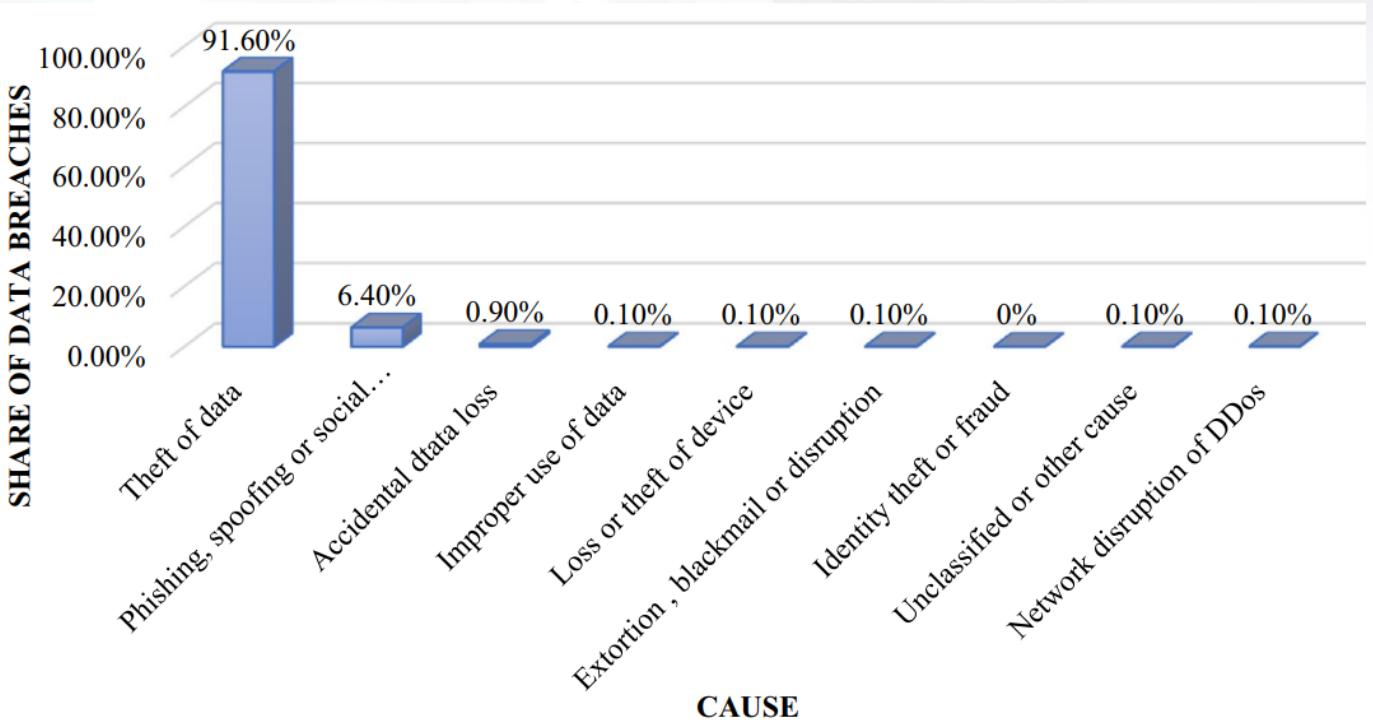
Cyber grooming

- Attacker establishes an intimate and emotional relationship with victim (mostly children and adolescents).
- Blackmailing, sexual abuse etc

Cyber stalking

- More strict form (a crime).
- Observing and harassing a victim continuously by means of electronic devices and other social media sites intentionally as part of a revenge, anger etc.
- It involves the invasion of a person’s right to privacy.

Leading Cause of Data Breaches



Thanks……