

InCyT Training Modules

Information Security for Employees

Unit no: (4) Week 8

Unit (Module) name: (Social Networking)

<i>Learning Activities</i>	☐ Webinar ☐ Exercises ☐ Workshop ☐ Presentation ☐ Other Streaming Webinar, Text, Self-assessment Exercises, Exercises with answers on discussion forums and within the organized sessions with trainer/mentor, e-portfolios
<i>Learning Responsible</i>	• David Sommer • Ileana Hamburg
<i>Learning Activity Goals</i>	1. Social networking roles 2. Functionality of social networking platforms 3. Security and privacy in social networks 4. Threats to online social networks and solutions to avoid them 5. Interdisciplinarity in social networks
<i>Skills to be Gained</i>	• TS3 Network security • TS4 Penetration (exploitable vulnerabilities) testing • TS5 Intrusion detection • SS3 Cognitive and behaviour analysis
<i>Duration of Learning activity</i>	2 weeks
<i>Learning requirements</i>	What is needed? • Internet access • Internet Browser • MS Office365

Brief information about the module

	Description
	Social networking helps people and organizations to connect with friends, are means of communication, help to launch a new business idea, sell products or services, and extend the reach of an own brand. Sure, there are also disadvantages of social networking like decreases face-to-face communication skills. Because organizations use intensively social media, attackers use trust and public nature of these platforms to attacks. Social networking security is important for business and private success so that training of employees like within this module can have a big contribution. The employees learn about such aspects by reading the corresponding text, watching streaming webinars, and solving exercises at own pace and reflecting about what they learn (e-portfolios). All the module documents are on the digital interactive project platform. The learners can test their answers on Self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forums and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the weekly meetings.

Content of the Learning Material

Introduction

Also due to growing technology, (online) social networks became very popular over the past few years. One reason is their ability to provide a platform for users to communicate with their family, friends, and colleagues.

Social networking refers to the use of internet-based social media sites for connection and communication with friends, family, colleagues, customers, or clients.

Social media helps people to have better relationships with family, friends, clients and mobile devices supporting social media are gaining more and more interest compared to other ways of internet access.

Social networks have their servers in data centres co-located, when possible, with major Internets Network Access Points (NAPs) where big Internet service providers connect to each other and where they provide the direct access to the Internet's fast connections.

Social networking roles

Social networking can have a social role, a business one, or both, by using sites like Facebook, Twitter, LinkedIn, and Instagram. Figure 1 shows some fields in which social networks play a role (Milsova et al.): entertainment, building business opportunities, making a career, improving social skills, and developing relationships with other individuals.

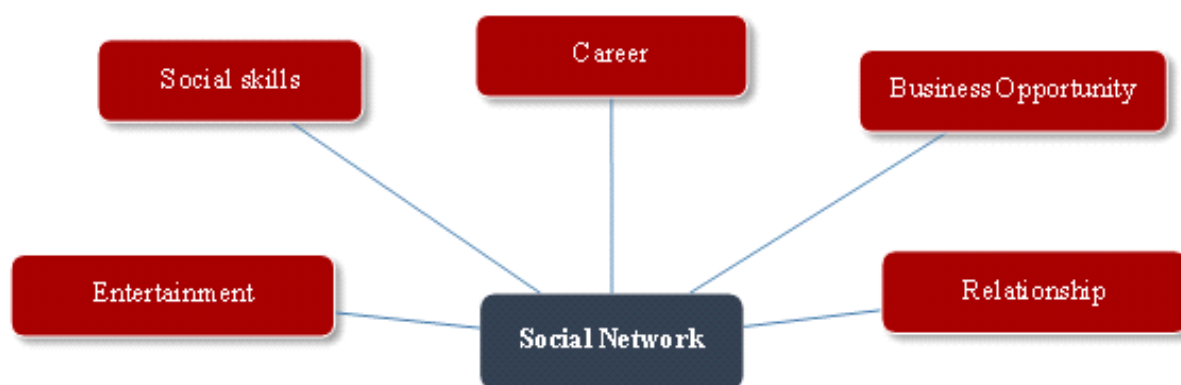


Figure 1: Social networks roles

Social networking is a base for marketers who seek customers. Marketers use social networking i.e. for increasing brand recognition and encouraging brand loyalty. Social media can help connect people and businesses and can help promote brand awareness. For example, a frequent Twitter user may learn about a company for the first time through a news feed and decide to buy a product or service. The company's chances of finding and retaining new customers increase through social networks. Marketers use social networking to improve conversion rates, provides access to and interaction with new, recent, and old customers. By sharing blog posts, images, videos, or comments on social media more people will visit the company's website and become customers. But there isn't a one approach to marketing strategies; every business is unique and has a different target demographic, history, and competitive marketplace. Because social networking companies want businesses to pay for their advertising, companies often restrict the number of reach businesses received through unpaid posts. For example, if a company has 500 followers, followers may not all receive the same post. The evolving nature of social networking makes it challenging to keep up with changes, and also influences a company's marketing success rate.

Facebook, Instagram, Facebook Messenger, and Twitter are the most popular social networking sites in the United States and also Europe. Others include Pinterest, Tumblr, Snapchat, TikTok, and YouTube, WhatsApp, Messenger by Google, and Tumblr. LinkedIn is another popular site, which helps connect professionals with co - workers, business contacts, and employers. Facebook remains the largest and most popular social network, with 2.91 billion people using the platform on a monthly basis, as of Dec. 31, 2021. Figure 2 shows number of users on platforms.

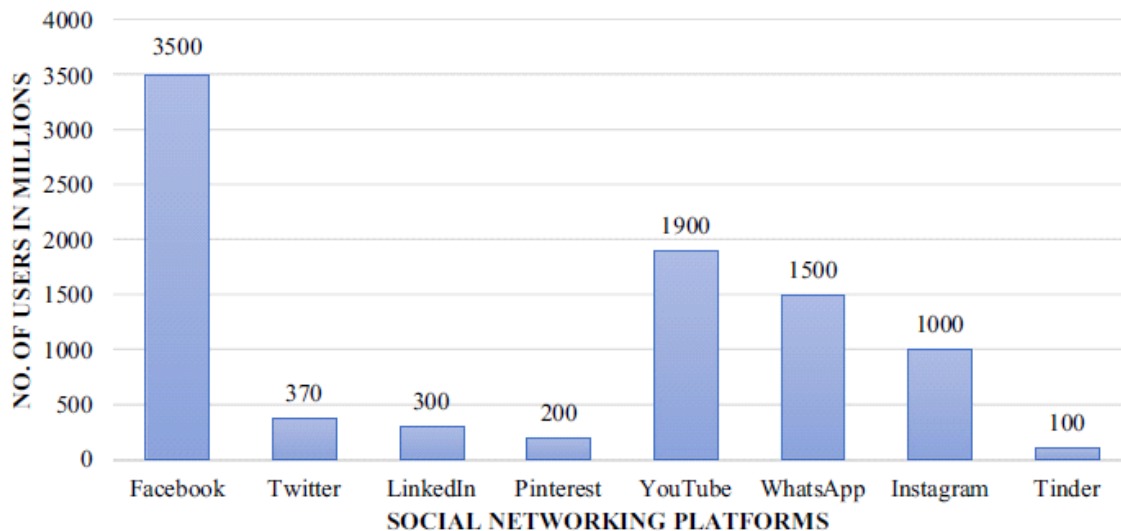


Figure 2: Number of users on platforms (<https://www.dreamgrow.com/top>)

Functionality of Social Networking

Social networking is based on the development and maintenance of personal and business relationships using technology by the use of social networking sites. These sites allow people and corporations to connect with one another so they can develop relationships and they can share information, ideas, and messages.

Family members who are far could remain connected through personal social networking sites like Facebook and share photos and send other messages from their lives. People can also connect with others (strangers) who share the same interests. Individuals can find each other through being members in groups, on lists, and the use of hashtags.

But there are also disadvantages related to social media, including the spread of misinformation and the high cost of using and maintaining social network profiles.

Each social network serves usually some specific use, but the functionality of these platforms is similar and can be classified into three main types:

- The networking functions serve to foster social relationships amongst users within the virtual platforms. In particular, they provide functionality for building and maintaining the social network graph.
- The data functions are responsible for the management of user-provided content and communications amongst the users. The variety contributes to the improvement (extended) of users' interaction and makes the platform more attractive.
- The access control functions aim to implement the user-defined privacy measures and to restrict unauthorized access to the user-provided data and information. Figure 3 shows the functionality provided by a typical virtual social network platform and provides more details (Cutillo et al. 2010).

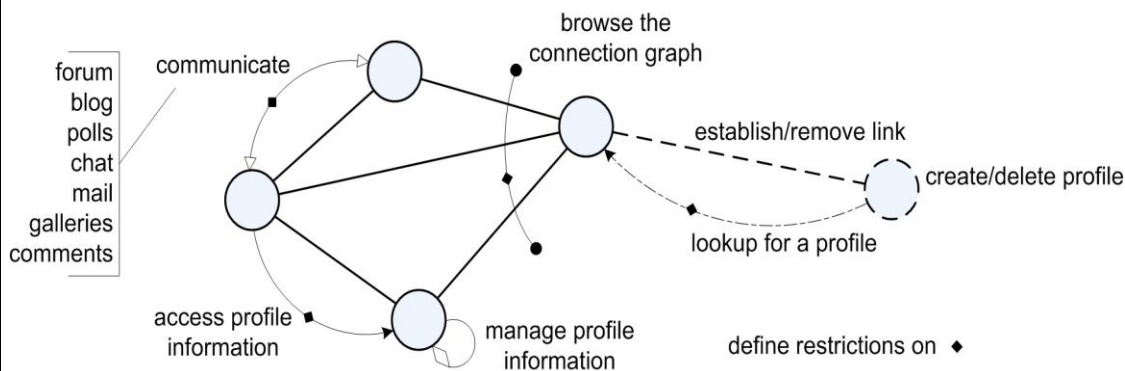


Figure 3: Main functionality of a typical social networking platform (<https://hal.archives-ouvertes.fr/hal-00687145>)

Social networking sites can be classified into ‘social connections’, ‘multimedia sharing’, ‘professional’ and ‘discussion forums’ (Figure 4 Jain et al., 2021)

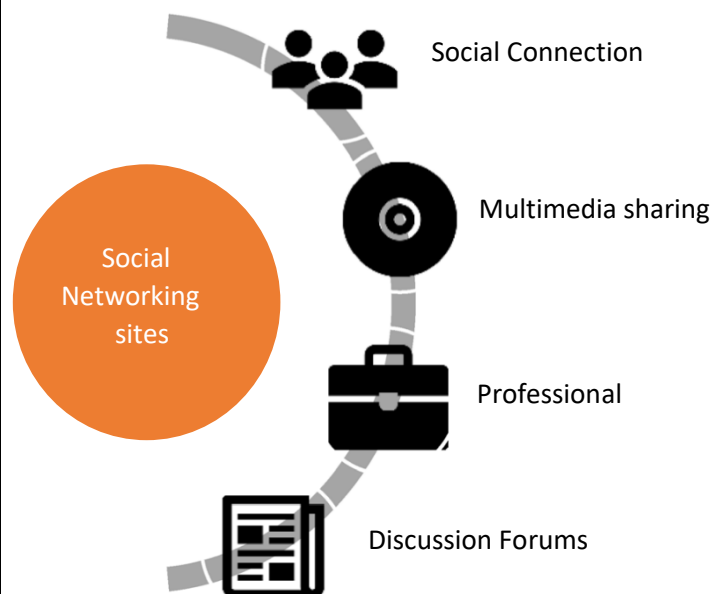


Figure 4: Social networking sites (Jain et al, 2021)

Advantages and Disadvantages of Social Networking

Social networking has the ability to affect both individuals and corporations—both positively and negatively and so it's important to take into consideration advantages and disadvantages of using such social media sites.

Advantages

Social networking allows individuals to keep in contact with family and friends they would otherwise not possible due to distance or lost touch. People can also connect with other individuals who share the same interests and develop new relationships.

Social networking allows companies to connect with new and existing clients. Companies can also use social media to create, promote, and increase brand awareness. They also rely on reviews and comments made by their clientele important for brand. It can increase sales and a higher ranking in search engines.

Social networking can help to establish a new brand. A company may use social networking to demonstrate its customer high service level and improve products and relationships with consumers. For example, if a customer complains about a product or service on Twitter, the company apologize, and take action to improve the situation.

Disadvantages

Social networking can contribute to the spread of misinformation Sahoo and Gupta, 2020 found that misinformation is 70% more likely to be shared than right information on Twitter.

Networking on social media can have detrimental impact on companies. Criticism of a brand spread very quickly on social media. This has disadvantages for a company's public relations (PR) department.

Social networking itself is free, but building and maintaining a company profile need hours of work and costs each week. Businesses need many followers before a social media marketing campaign starts generating a positive return on investment (ROI). For example, submitting a post to 15 followers does not have the same effect as submitting the post to 15,000 followers.

Security and privacy in social networks

The information shared in social networks and media spreads very fast, which makes it attractive for attackers to gain it. There are security and privacy issues related to the user's shared information when a user uploads personal content such as photos, videos, and audios. The attacker can maliciously use shared information for illegitimate purposes.

Some different security and privacy threats and existing solutions that can provide security to social network users are shortly presented.

Due to intensive use of technology, interactions have been extended through internet. Unfortunately, lack of awareness among users regarding security and privacy has the potential to lead to various cyber-attacks through social media. The threats which users detected from the beginning of social networks can be divided into three categories i.e., conventional threats, modern threats, and targeted threats (Fig. 5, Jain and Gupta, 2018). Conventional threats include threats that users have been experiencing from the beginning of the social network. Modern threats are attacks that use advanced techniques to compromise accounts of users and targeted attacks are attacks that are targeted on a particular user which can be committed by any user for varied personal vendettas.

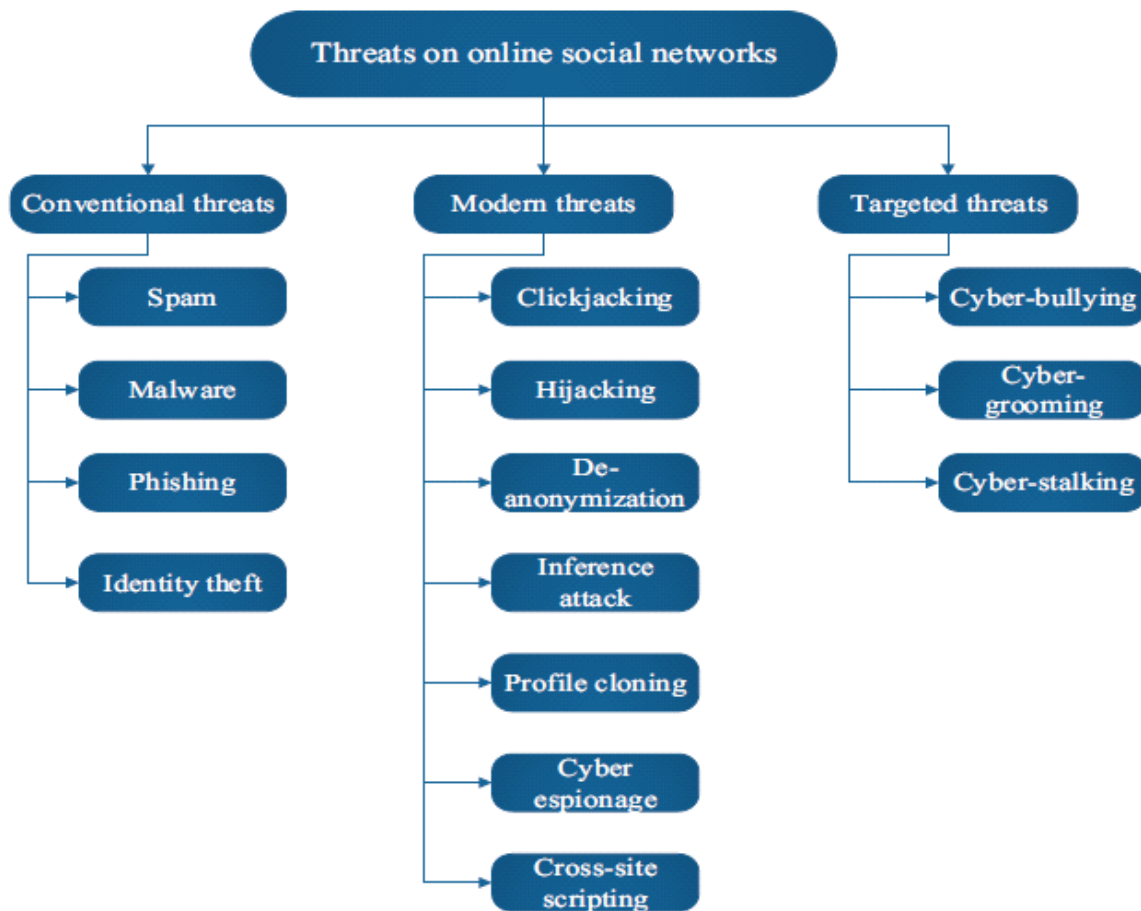


Figure 5: Classification of threats (Jain et al, 2018)

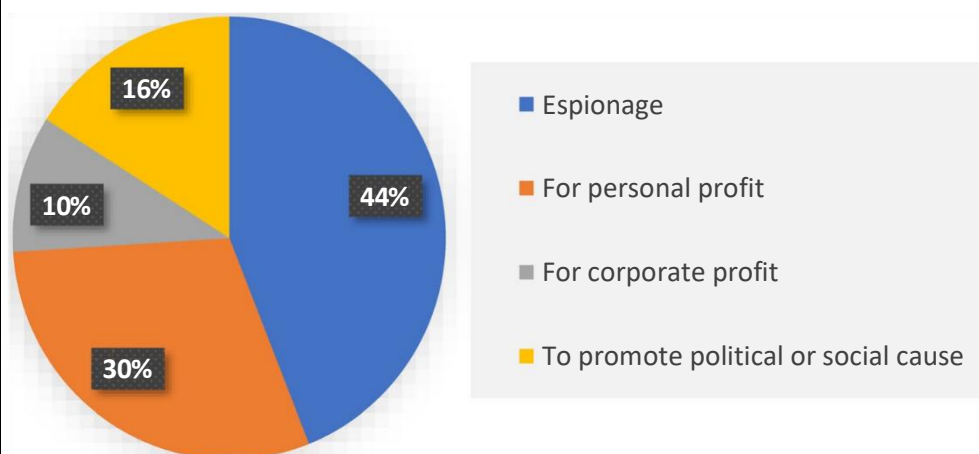


Figure 6: Most types of hacking in 2021 (Jain et al, 2021)

Solutions to threats

Researchers in academia and industries try to find solutions for the threats in social networks for different types of hacking like shown in Figure 6. Solutions and some approaches have been proposed and could be

classified into two groups: social network operator solutions and academic solutions (Jain et al, 2021). Figure 7 shows the classification. A short description is presented below.

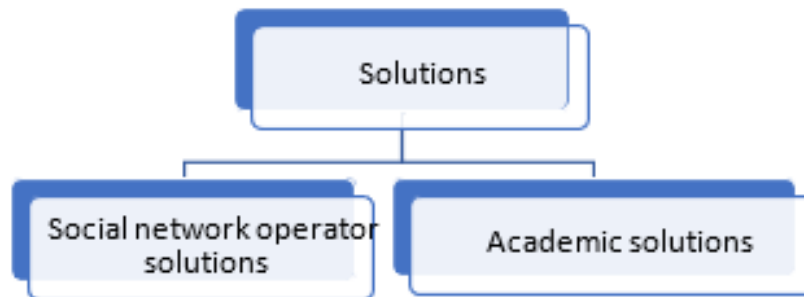


Figure 7: Classification of solutions to threats (Jain et al, 2021)

Social network operator solutions

Authentication mechanism

To make sure that only a legitimate user is logging or registering in a social network and not a social Bot, authentication procedures such as CAPTCHA, multi-factor authentication, and photos-of-friend identification have been proposed. For instance, social networks like Twitter and Facebook use two-factor authentication principles. This principle uses a login password and a verification code received through a mobile device. This helps to mitigate the risk of an account being compromised and prevents an attacker from hijacking a legitimate account and posting malicious content.

Security and privacy setting

Many social networking sites provide configurable security and privacy setting to empower the client to put personal information from undesirable access by outsiders or applications. For instance, the Facebook client can modify their security setting and select the audience (like friends, friends of friends, and everybody) in the network, who can see their details, pictures, posts, and other sensitive information.

Report users

Social networks protect people from attacks by providing the facility to report any form of abuse or policy violations by any user in their network. For instance, if a user sees something on Facebook that correspond to the individual's sentiments, but it doesn't violate the Facebook terms, then the user can utilize a report (links) to send a message to the one who posted it asking him to take it down or remove. When Facebook receives a user report, it is reviewed and removed according to the Facebook community standards.

Academic research-based solutions

Phishing detection

Phishing worried the privacy and security of many traditional web applications such as websites, social networking sites, emails, and blogs. Consequently, several anti-phishing techniques have been developed to detect phishing attacks. For instance, Aggarwal et al. proposed the PhishAri technique for real-time identification of phishing attacks occurring on Twitter. It utilized specific Twitter features like account age and number of followers to detect if the posted tweet is phishing or safe.

Cyberbullying detection

Cyberbullying is the use of electronic media such as emails, chats, phone conversations, and online social networks to oppress a person. Unlike traditional bullying, cyberbullying is a continuous process maintained through social media. Although detecting cyberbullying is more complex than detecting racist language and spam, some researchers have tried to detect it using more complex document representation and additional information about victims and bullies. Machine learning techniques can be applied to detect cyberbullying.

Clickjacking

An automated system can analyse web pages to protect the user against clickjacking attacks. It consists of a code that can detect overlapping clickable elements. And in addition to this solution, they also adopted the NoScript tool, which has an anti-clickjacking feature included in it.

Cyberstalking

Encryption techniques are available for devices on recent versions of Android and iOS. If a device is stolen, the thief cannot read the contents if encryption is enabled. Further, any attempts to read the information from internal or external memory is thwarted by the existence of a device password. There are various technologies which can be used against stalkers like smartphone fingerprint lock.

Spam detection

A framework called Spam Spotter can help against a spam attack on Facebook. It is based on the intelligent decision support system (IDSS). It gathers all relevant information from the user profile with the help of a decision process in IDSS and then analyses it by mapping user data to the classification of a user profile as a spammer or legitimate.

Malware

Cross Site Scripting Worms (XSS worms) are malicious programs that propagates through visitors of a website hopping to infect other visitors progressively.

The worm propagates slower when members mostly visit their friends rather than strangers. It can also be slowed down by the clustered nature of social networks.

Although academia developed such innovative solutions to address the security measures in connection with social network security, they lack real-world implementation and feasibility. Thus, there is an urgently need

to continuously and iteratively review security issues in social networks taking into consideration technological developments.

Interdisciplinarity in social networks

The interdisciplinary field referring social networks is social network analysis (SNA) and include insights from other social science disciplines such as sociology, anthropology, psychology, communication, and others. SNA is part of an even larger interdisciplinary field in charge of studying all types of networks called network science which includes work in physics, computer science, data science, biology, engineering, mathematics, and other fields. The relationship between these fields is showed in Figure 8 (<https://bookdown.org/omarlizardo/main/1-2-what-is-a-social-network.html>).

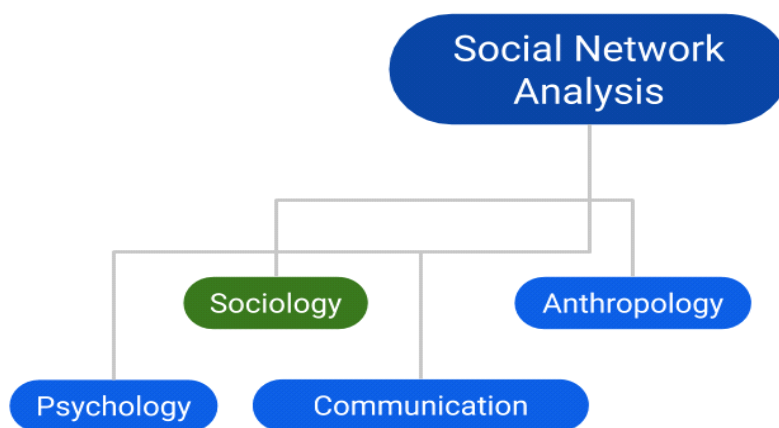


Figure 8: Relationships between fields in SNA (<https://bookdown.org/omarlizardo/main/1-2-what-is-a-social-network.html>)

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. Social networks roles
2. Social networking sites
3. Interdisciplinary fields in connection with social networks

Attachments:

1. Presentation
2. Video movies

References:

References

- Aggarwal A., Rajadesingan A & Kumaraguru P. (2012). PhishAri: automatic realtime phishing detection on twitter. eCrime Res. Summit, eCrime. 1–12.
- Ankit Kumar J., Somya Ranjan S. & Kaubiyal J. (2021). Data breach causes worldwide. URL: <https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/>
- Cuttillo, A., Manulis, M. & Strute, T. (2010). Security and Privacy in Online Social Networks. EUROCOM. TU Darmstadt.
- Gupta B. & Sahoo, S. (2021). Online social networks security: principles, algorithm, applications, and perspectives. CRC Press.
- Jain A. & Gupta B. (2018). Detection of phishing attacks in financial and e-banking websites using link and visual similarity relation. Int J Inf Comp Secur 10(4):398–417.
- Jain, A., Sahoo, S.R. & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex Intell. Syst. 7, 2157–2177.
- Kangur, K. (2022). The 15 Biggest Social Media Sites and Apps. URL: <https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/>.
- Mislove A., Viswanath B., Gummadi K. & Druschel, P. (2010). You are who you know. In: Proceedings of the third ACM international conference on Web search and data mining—WSDM '10, 251.
- Rydstedt, G. (2018). Clickjacking – OWASP. URL: <https://owasp.org/www-community/attacks/Clickjacking>.
- Sahoo SR, Gupta BB (2020). Fake profile detection in multimedia big data on online social networks. Int J Inf Comput Secur 12(2–3), 303–331.