2025

Privacy and Security in Social Media - I

Dr. Babasaheb Ambedkar Open University

Course Writer, Editor & Reviewer

Prof. (Dr.) Nilesh Modi
Professor and Director,
School of Computer Science,
Dr. Babasaheb Ambedkar Open University,
Ahmedabad, Gujarat

ISBN:

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyright's holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

BAOU
Education for All
Dr. Babasaheb
Ambedkar Open
University

BSCCS-305

Privacy and Security in Social Media - I

BLOCK – 1
FUNDAMENTALS OF SOCIAL MEDIA

UNIT- 1
SOCIAL MEDIA
PASTS & PRESENT

1.1 *OBJECTIVES*

After successful completion of this unit, you will be able to-

- Understand the fundamentals, evolution and trends of social media.
- Understand the current scenario of social media.
- Define the impact of social media on business.

1.2 INTRODUCTION

Isn't "Social Media" the most used phrase and you keep hearing about it every minute, in today's computer era? Yes, social media is that recurring expression in our life which we speak around a lot often to describe what we post and read on sites and apps like Facebook, Twitter, Instagram, Snapchat and others. So, that makes us simply infer that social media are/is web -based sites that allow people to interact with each other.

Though, social media gets very confusing too sometimes, when we have to describe and talk about certain sites like Facebook, and also a site like Digg, plus a site like Wikipedia, and even sometimes a site like I can have Cheez burger. You look at these sites, and say to yourself, just what exactly is social media, anyway? The term is so vague that it can basically be used to describe almost any website on the internet today. But, then is that right?

Some people have more of a restricted view of social media, often equating it to mean the same as social networking (a.k.a. Facebook, Twitter, etc.). Other people don't consider blogs to fall under the social media category. Some people even consider a simple question & answer (Q&A) website like Quora.com to be a social media platform. It seems as if everyone has their own personal opinion of what social media is and isn't. But, can that establish the actual definition and standards of social media? No.

Hence, let's dive deeper into the general concept of social media to gain a clearer and more precise understanding. To get away from the complicated jargon and stick to simpler and clearer understanding, we will break the phrase "Social Media" into two parts:

The 'social' part: refers to interacting with other people by sharing information with them and receiving information from them.

The 'media' part: refers to an instrument of communication, like the internet (while TV, radio, and newspapers are examples of more traditional forms of media). From these two separate terms, we can pull a basic definition together- “Social media are web- based communication tools that enable people to interact with each other by sharing and consuming information”. Let’s see figure describing the essential vast landscape of social media.

1.3 *HISTORY OF SOCIAL MEDIA*

If you think of it, fifty years ago, no one would have known of “Social Media”. But now, everyone knows about it. This term has become a common knowledge in society especially for the youngsters. It is not just limited to being some knowledge that generally goes unpracticed, but is rather the most popular pursuit of this digital age. It is a new mode of entertainment and where people can share and exchange their thoughts (through what most of us know as posts / statuses), personal information, photos and other media.

This media is apparently growing bigger and bigger every day with more and more people using it across the globe and also promoting the usage and its positive effects to the people they know in their circle.

New and more advanced social media platforms are created every year with more interesting things that can be offered to internet users. Now, to look at it, there are so many known and followed social media platforms like Blogger, MySpace, Facebook, Twitter, Pinterest and more.

Let’s discuss a brief history of social media-

In 1978, the first social media was created. Bulletin Board System (BBS) was created by Ward Christensen and Randy Suess to announce meeting and sharing information by posting it on BBS. It was the beginning of virtual community and the first dial-up in history.1995 was the year for personal websites. After internet (WWW) launched and loved by many people, Geocities a web hosting service launched by Beverly Hills Internet (BHI). It allowed internet users to create simple websites for themselves.

Social media service that appeared in 1997 was SixDegrees. SixDegrees lets its users to create profile and list of friends. It was used by 1 million users. 1999 was the year for Blogger and Live journal. Users could write, share and communicate with friends by using their own blog or journal. Friendster was launched in 2002. It could be included in the social networking group. It lets users to create profile and virtual connection with people around the world. Now, Friendster has become a social media for games.

Myspace, LinkedIn and WordPress were launched in the year 2003. Most of Myspace users were musician and band. WordPress was created to be used as open-source content management system and LinkedIn was launched as business-oriented social networking.

In 2004, Mark Zuckerberg launched ‘Facebook’. In the beginning, Facebook was created as social networking for college students. YouTube was launched in 2005 and founded by former employees of PayPal Jawed Karim, Steve Chen and Chad Hurley. It is a social sharing that let users freely upload and share a video. Launched in 2006, Twitter is known as social networking and microblogging site. Users can share and exchange 140-character messages. This short messages are called as tweets. In 2011, Google launched new product of social networking, Google plus (Google+). Google plus let you have video chat (hangout) and exchange information. In 2012, the first social scrapbooking that gained 10 million users faster in history launched. This social scrapbooking, Pinterest helps you create and share album of photos. New and more advanced social media platforms are created every year with more interesting things that can be offered to internet users. Now, to look at it, there are so many known and followed social media platforms like Blogger, MySpace, Facebook, Twitter, Pinterest and more.

1.4 SOCIAL MEDIA TRENDS

In this section, we will discuss about the current trends in social media. If we take a look at it, we see that social media trends follow movements in culture. These social media movements reveal key influencers of consumer behaviour and provide a powerful platform for testing the marketing innovations and brand ideas. Statistics shows that today, 2.46 billion people are active on social media. Some top social media trends are-

Ephemeral content -

Ephemeral content flashes across the internet for a second, maybe 24 hours, and then it’s gone. But when done well, it leaves a buzzing trace across people’s memories and brings lasting benefits to your company. These content blips are the basis of Instagram and Snapchat stories, where millions of users have become seduced by quick-fire content. One advantage is posting without polishing. People can easily upload a raw photo or video without fussing about editing. It’s spontaneous, authentic, in-the-moment storytelling. It gives marketers a savvy way to test concepts quickly. The numbers speak for themselves. As of November 2017, Instagram Stories topped 300 million daily users, while Snapchat had 187 million people sending fleeting messages every day, and when that many eyes are in one place, businesses take note. Last year, Instagram had more than one million advertisers using Stories each month. Ephemeral content is booming because it taps into “now culture.” Watch it now, share it now, and experience it now.

Live streaming-

Video lets you experience events in your own time. Live streaming lets you do this in real-time, so everyone can be there even when they’re not. With recent success stories like Periscope, Twitch, and Facebook Live climbing aboard YouTube’s gravy train, the video streaming market is on track to be worth $70 billion by 2021.

Teaching online classes, broadcasting an event, doing a live demonstration of a new product—all of these are ripe for live streaming. It’s a pure, immediate, and relatively effortless way to reach audiences and make them feel part of the experience. It also feeds into our “now culture” syndrome. Since, all major social media platforms now offer live streaming, it is expected that this social media trend will continue to rule beyond 2019.

Chatbot conversations-

Chatbots are taking over the web. Facebook Messenger recently announced that there are now more than 30,000 active chatbots gathering information, giving product guidance, and taking orders, and you better get ready for more. Gartner estimates that by 2020, 85% of our engagement with businesses will be done without interacting with another human.

Why the chatbot frenzy?

Chatbots are efficient. They provide faster response times for customer success, easier reservation services, and seamless bill paying at scale. And all without completely sacrificing that human touch—Facebook reports that 56% of people would rather message than call customer service.

The rise of augmented reality-

Picture this: a full 3D scan of your body, uploaded to Snapchat, and dancing to Madonna's Vogue. Augmented reality has quite literally changed the way people experience the world. It may have started with people searching street corners for Pokémon. But that was just the beginning. By enhancing real world experiences, AR lets people connect with brands through a heightened level of immersion. And companies are taking note.

According to a Deloitte survey, nearly 90 percent of companies with revenues between $100 million and $1 billion are already using AR as part of their business. The Apple iPhone 8 and iPhone x are both equipped with a chip that offers AR experiences. And platforms like Google Glass and Snap Chat's Lens Studio make is easier than ever to augment your reality.

Furniture and meatball retailer, IKEA, is one of them. Their new IKEA Place app lets you add a digital layer of furniture right on top of your real living room—so you can test styles, colours, and fabrics without opening a single box.

Experimentation-

This is one trend that's here to stay: learning how to keep up with the mind-blowing pace of social media change. Instagram Shopping, Twitter's character increase, Facebook's algorithm updates, LinkedIn's native video—that's a tiny fraction of the social media changes launched in 2018. Can you keep up with it all? Probably not. But having an agile approach and an open mind is a good place to start. To stay relevant on social media, move with the change, learn fast, and never stop experimenting. And beyond the trends, remember why you're on social media in the first place: to build emotional connections with your customers and bring them closer to your brand.

1.5 CURRENT SCENARIO OF SOCIAL MEDIA

In today's fast paced world, there are so many burning issues around us which we need to think upon and act, it's an alarm for us to be aware about the society and current issues like abuse of human rights, education, corruption by political leaders, crime against women, bribery, misinformation to consumer, etc. need to be discussed openly in an effort to do something about it and bring a revolution. Social media provide a platform for discussion on such issues.

Nowadays, social media are used by most of the political leaders in India. For instance, our Prime Minister tweets regularly on daily issues on Twitter Apps. Social media plays a great role as information source for travelers.

1.6 *IMPACTS OF SOCIAL MEDIA ON BUSINESS*

Advances in technology always changes business perspective, today's market leaders are harnessing new technology to sharpen their marketing strategies and trying to reach more customers. The business world now relies on the internet for much of its communications, marketing or otherwise. Almost all companies have their Facebook accounts, and individual leaders of companies have separate individual accounts on Linked in, Twitter, Instagram, and other social media sites.

New social media sites are popping up almost every week. Social media has created a business climate in which thousands of impressions can be made with one social media post. That impression could be positive or negative. we always have to careful about it. Within social media, individuals also developed audiences in the millions who follow their posts every day. Social media is a hugely powerful tool for marketing. There are several powerful tools, one such is "blog" too.

Blogs provide marketers real-time dialogue with customers and an approach to promote their products or services. A blog is an online journal with regularly updated content. This content is pushed to subscribers by RSS (Really Simple Syndication) or e-mail and allows for response and discussion from site visitors. RSS enables users to automatically gather updates from various websites, especially news sites and blogs, and display headlines and a brief summary of those updates in a single location.

Blogs can be considered to be offerings of social media unless the site is actually part of the company's main web page. Well-run marketing blogs usually focus tightly on one peak area or product line. The aim is to provide the blog readers with a constantly renewing source of news and insight about that particular topic.

It has its own challenges, because the social media platforms are continuously changing and evolving.

Also, the audiences being reached often read (or view) and believe the messages seen on various social media platforms without understanding the context of the message. A social media post that goes viral can become the cause of closing down a business, even if the post is not true.

So, that we can say the social media is the newest challenge/opportunity for marketers. Companies that want to retain market share and build their image must develop tactics for the use of social media and for defending against problems created by the use of these powerful marketing tool.

1.7 CHECK YOUR PROGRESS

- What do you mean by social media? Explain how is it beneficial for society?
- Why is social media really important for business? Justify.
- Discuss the evolution of social media across the globe.
- Discuss the top five social media trends today.
- How social media can express your image/reputation negatively?

UNIT- 2

SOCIAL MEDIA IN INTERPERSONAL COMMUNICATION

2.1 OBJECTIVES

After successful completion of this unit, you will be able to-

- Define e-communication tools.
- Understand the importance of interpersonal communication.
- Define the role of social media in communication.

2.2 INTRODUCTION

E-communication, or electronic communication, refers to the transfer of writing, signals, data, sounds, images, signs or intelligence sent via an electronic device. Some examples of e-communication are email, text messages, social media messaging and image sharing. E-communication is a common form of interaction for many people. The use of e-communication allows people to interact in different ways and combine many forms of media in the process. E-communication makes it easy to interact with groups through chat interfaces or video conferencing. Companies use electronic communications to enhance their business and to avoid obstacles, such as long-distance communication with their clients or partners.

Social media are computer-mediated technologies that allow individuals, companies, NGOs, governments, and other organizations to view, create and share information, ideas, career interests and other forms of expression via virtual communities and networks. In other words, we can say that social media uses web-based and mobile technologies on smartphones and tablet computers to create highly interactive platforms through which individuals, communities and organizations can share, co-create, discuss, and modify user-generated content or pre-made content posted online. The variety of stand-alone and built-in social media services currently available. Social media changes the way individuals and large organizations communicate. Social media are interactive and Internet-based applications, user-generated content such as text posts or comments, digital photos or videos, as well as data generated through all online interactions. social media facilitate the development of online social networks by connecting a user’s profile with those of other individuals or groups.

2.3 TYPES OF E-COMMUNICATION

Internet provides many effective communication tools, including e-mail, mailing lists, discussion groups, chat services, web conferencing, blogs, and RSS feeds. In recent years, social networking sites such as Facebook and Twitter have also joined the mix look of e-communication. These various tools allow you to communicate one-to-one or one-to-many, depending on your communication needs. They also enable communication locally between people who know one another or worldwide with people who share common interests. There are several types of e-communication-

E-mail-

E-mail is one of the most popular e-communication tools over the internet. E-mail allows you to send messages to one person or simultaneously to a group of people. E-mail is convenient and widespread to use. We can connect from anywhere and anytime with the help of internet service. Most people have at least one e-mail address.

In order to send e-mail, you must know the recipient's e-mail address. E-mail addresses consists of two parts: a username and a domain name. The username refers to the mailbox name or login name or user ID. The domain name is the internet address of the computer where the user's e-mail is stored (also called the mail server). The parts are separated by an @ symbol. For example, the e-mail address for the school of vocational studies is vocschool@uou.ac.in (this is an example only). There are many e-mail services available, which are free to use (partial free). you may create your own e-mail id from the following. e.g. Microsoft Outlook, Gmail, Yahoo! Mail.

Mailing Lists-

Mailing List is another form of e-mail, which can involve just a few people or thousands of people. Mailing lists distribute information to an e-mail subscription list. Many companies and professional organizations rely on mailing lists to distribute their information. Postings, in the form of e-mail messages, are automatically delivered to your e-mail. You can simply read the contents of the messages. Subscribing to a mailing list involves sending a message to the list’s administrator.

Discussion Groups-

Sites such as Yahoo! and Google allow users to create and join online discussion groups. Discussion groups are also referred to as forums or bulletin boards. These function very much like mailing lists except they are easier to create and maintain. They are also less invasive than mailing lists since you go to a website to view and post messages. Discussion groups work very well for communication among local interest groups and clubs. Within a discussion group, a discussion on a particular topic is often called a “thread.” To start looking for other discussion groups, try Yahoo! Groups or Google Groups.

Social Networking-

As information technology expanded, new social networking sites have developed on the internet. Social networking sites allow users to share their information through various mediums, as- text, audio, video, pictures, animations and info graphics. Social networking is a way of communication by email or instant messages within the website, and develop networks of friends or associations. Popular social networking sites include Facebook, Twitter, Google+, and YouTube. Nowadays, large corporations have become more attracted to social networking sites because of advertising revenue and the ease of marketing products and services.

Facebook-

Facebook is the world’s largest social network, provides a place for social connection via sharing of photos, videos, and text updates. Users can create personal profiles and establish relationships with other people and companies. Facebook was founded in 2004 by Mark Zuckerberg and his roommates at Harvard University. The Facebook membership is free to anyone over the particular age.

Twitter-

Twitter launched in 2006, is a “microblogging” platform that allows users to communicate through brief messages (known as “tweets”), limited to 140 characters. The original idea behind Twitter was for users to post messages in response to the question, “What are you doing?”

The prompt has since been changed to the more generic “What’s happening?”, but users can post anything that’s on their minds, and often use Twitter as a way to share links to websites, photos, videos, and other web-based content. Twitter employs a convention called a “hashtag,” which is a word or phrase immediately preceded by a # (Hash) symbol. By placing a # symbol in front of a word in a tweet, the word is automatically turned into a hotlink which, when clicked, will perform a search of recent tweets containing that word. The ability to group together tweets containing a particular word or phrase has contributed to a phenomenon known as the “internet meme.” A meme can be a word, phrase, idea, image, video, or anything that spreads very rapidly via Twitter or any other means of internet communication.

Google+ (Google Plus)-

Google Plus was launched by Google corporation in year 2011 as an attempt to compete with Facebook. Features of Google+ include “Circles” for sharing information with different groups of people (like Facebook Groups), and “Hangouts” for video chatting with a friend or groups of friends. Google Hangouts recently merged with Google’s Talk program, which created a single location for all text, video, and image sharing between a friend or a group of friends.

Tumblr-

Tumblr launched in year 2007, is another “microblogging” platform that gives users a quick way to post text, images, audio, video, links, and quotes in a community setting. Unlike regular blogs, Tumblr blogs (also called “Tumblogs” or “Tumblelogs”) are frequently used to share the author’s creations, discoveries, or experiences while providing little or no commentary.

YouTube-

YouTube began in year 2005 and has grown exponentially since then. It is another key product of Google corporation. Users may register with YouTube to upload videos, rate them and participate in different user groups, but it is not necessary to register in order to view video clips, send them to others, or embed them in other websites.

Instagram-

Instagram is a photo sharing application launched in year 2010 that allows users of mobile devices to take a photo, apply a digital filter to it, and then share it on a variety of social networks. A distinctive feature confines photo to a square shape, similar to old-fashioned Kodak Instamatic and Polaroid images. In 2012, Facebook acquired Instagram and independently managed.

Pinterest- Pinterest launched in the year 2010, is currently one of the fastest growing social networks on the web. Pinterest allows users to create and manage theme-based image collections by uploading their own photos, or by importing (also known as “pinning”) images from elsewhere on the web. Users can browse and/or “follow” other pin boards for inspiration, and can “like” and/or “re-pin” images to their own collections. Users can also share their “pins” on both Twitter and Facebook.

Flickr-

Flickr is an image and video hosting website and online community launched in year 2004 and acquired by Yahoo! in year 2005. The service is widely used by bloggers to host images they embed in blogs and other forms of social media.

LinkedIn-

LinkedIn launched in the year 2003 as a social networking tool for work professionals, has become the standard for employers looking for new talent. Through LinkedIn, users can search for jobs, submit applications, and join work-related groups.

Foursquare-

Foursquare is a location-based mobile application that combines aspects of social networking and gaming.

MySpace-

MySpace launched in the year 2003, was the most popular social networking site in the world around the year.

Social Bookmarking-

Social bookmarking is a method for internet users to organize, store, and share links to online resources. Prior to the proliferation of social bookmarking services, the only way for internet users to save (or “bookmark”) links to web content that interested them was to add them to a list of favorite links stored on their computers. If they typically use more than one computer (one at home and one at work, for example), they had to go through the inconvenience of saving their favorite links on both machines. Social bookmarking sites now enable users to gain access to their favorite links from any device with an internet connection, and to share links with other users.

Internet Chat-

In Internet chat, people view and respond to messages from one another instantaneously, much like a telephone conversation. Although some chat software includes audio and/or video aspects, most chat and instant messaging programs are text-based. One person types a message on the screen, and the other person sees the message either as it is being typed or immediately after it has been typed.

There are two forms of internet chat frequently found on the web: chat rooms and instant messaging. Chat rooms tend to be open forums where a number of people chat with one another simultaneously. Often the people who meet in a chat room are people that have not met each other in the "real world." Instant messaging (IM), on the other hand, is a one-on-one form of internet chat. Although you can choose to instant messaging with strangers, often it is used to communicate with friends and family. Examples of instant message services include AOL Instant Messenger, Yahoo! Messenger, Facebook instant messaging service, etc.

Web Conferencing-

Web conferencing is currently being used by businesses for employee training, meetings, and general communication. Educational institutions use web conferencing to enhance onsite classes or distance education classes. Popular conferencing programs include AnyMeeting (a free service for hosting meetings of up to 200 participants), and fee-based services Elluminate and GoToMeeting, which provide programs specifically designed for businesses and educational institutions.

Blogs-

A blog is a kind of website that allows a web author to simply and easily share thoughts and ideas with other web users. The word blog comes from weblog, which refers to a log of dated postings by a particular author or group of authors. Blogs can cover any topic or can just be someone’s daily, weekly, or occasional diary of thoughts and opinions. Blogs can be interactive when readers add comments and a discussion is created. You can also, create your own blog. There are many software programs and web-based blog hosting services, some of which are free, such as Blogger and WordPress. Blogs are created using a simple-to-use content management system.

2.4 INTERPERSONAL COMMUNICATION

Interpersonal communication skills are essential for developing other key life skills. Interpersonal communication is the exchange of information between people. This is not just limited to verbal communication but instead includes body language and facial expressions as well as textual communications and other interactions that are mediated by technology in some way. Good interpersonal communication skills enable us to work more effectively and efficiently in groups and teams. It is often desirable to build strong relationships with others, which can in turn lead to better communication and understanding. Interpersonal communication can serve many advantageous purposes. It allows us to influence the behavior, attitudes, and opinions of others. In other words, we can say effective interpersonal communication in the workplace is integral to a well-functioning, high-performing team. Interpersonal skills are the ability to communicate important information and manage social interactions with colleagues, both up and down in the business. There are certain skill sets that are crucial for professional life as well as for personal life to be able to exercise in their routine environment. Regardless of your workplace, interpersonal skills are important. Some of the key interpersonal communication skills are-

Exercising Self-Awareness- Self-awareness falls within the realm of emotional intelligence. Emotional intelligence is comprised of four primary components, i.e. Self-awareness, Emotions, Empathy and Relationship building.

Being Cognizant of Nonverbal Communication- Some forms of nonverbal communication include- e. g. Eye contact, Facial expressions, Body language, Gestures, and Physical contact (such as shaking hands, touching an arm, pushing, etc.).

Being Respectful of Others-

Showing Empathy and Understanding- Empathy, along with active listening and strong communication skills, also is useful in terms of negotiation tactics.

Being a Clear Communicator- Communication is an important part of life, as well as a necessary component of any personal or business relationship.

Engaging in Active Listening

Behaving Appropriately- Some universally accepted behaviors should be exercised by everyone, e. g. Being punctual, showing courtesy, being cooperative and easy to work with, having a positive attitude, dressing appropriately, etc.

2.5 ROLE OF SOCIAL MEDIA IN COMMUNICATION

The role of social media in communication is immense, because of its extensive and convenient approach. The social media is not limited till the communication purposes only, but also performs key role in digital marketing and becoming a strategic tool in terms of building brand awareness and running a marketing campaign. Shifting from the era of conventional or mass media, by using social media and digital marketing, marketers can track brand's competitors and have more measurable campaign results. Digital communications media are inherently capable of being more interactive, participatory, decentralized, and less hierarchical. As such, the types of social relations and communities which can be built on these media share these characteristics. There are some benefits of digital communication-Communication is instant and fast-paced, Communication is extensive, Communication is convenient and Communication contributes to positive social change.

2.6 SOCIAL MEDIA A GOLDEN BRIDGE FOR COMMUNICATION

We look around and find that Internet and digital technologies are revolutionizing our lives. This world appears to be a highly privileged place where people interact with each other, search for information online, buy goods and services. What were once known as traditional advertising techniques have now been significantly transformed. We remember the time when advertisement used to be limited to the selected media- e.g. TV, radios or movies. Now it has conquered new spaces with social networks. Indeed, in 2018, 40.2% of ads that the masses had seen were digital. Social networks has emerged as one of the most important areas of interest, acting as broadcasting and marketing tools for companies to promote their business and also carry out customer care.

Since, advertising has taken social media, the most exposed are the millennials –people born in the 21st century and reaching young adulthood. They have a strong relationship with social media. Comments and recommendations are very important to them. According to a Hubspot study, 71% of the millennials are more likely to buy a product if it has been recommended online.

2.7 CHECK YOUR PROGRESS

Part- A (Fill in the blanks and True/False type questions)

a) BBS stands for............

b) BHI is abbreviated as.............

c) The full form of AR is.............

d)................is a piece of software responsible to conduct a conversation through auditory or

textual methods.

e) ....is a subscription-based market research company that provides insights and trends related to digital marketing, media, and commerce.

f) Ephemeral content is a content that resides across the internet for a long period of time. (True/False)

g) General Data Protection Regulation (GDPR) aims to protect the data and privacy of individuals in the Asian Region. (True/False)

h) Social media are web-based communication tools that enable people to interact with each other by sharing and consuming information. (True/False)

i) In 2006, Mark Zuckerberg launched ‘The Facebook’. (True/False)

j) Google launched new product of social networking named Google plus (Google+) in 2011. (True/False)

Part- B (Descriptive type questions)

- What do you understand by e-Communication? Discuss its various modes?
- Social media plays a very important role in our daily lives and in interpersonal communication. Discuss in your own words.
- Social media acts as a golden bridge for communication. Comment.

Answers- (Part A- Fill in the blanks and True/False type questions)	
(a) Bulletin Board System	(b) Beverly Hills Internet
(c) Augmented Reality	(d) Chatbot
(e) eMarketer	(f) False
(g) False	(h) True
(i) False	(j) True

UNIT- 3
Social Media, Ethics and the Privacy Paradox

3.1 OBJECTIVES

After successful completion of this unit, the learner will be able to-

- The concept of social media and describe its evolution and role in modern society;
- Identify the major social media platforms and explain how they facilitate communication and information sharing;
- Understand the nature of personal data shared on social media and how such data can be collected, stored, and reused;
- Concept of privacy in the context of social media and the digital information age;
- Common privacy risks and security threats associated with social media use, especially among children and adolescents.

3.2 INTRODUCTION

The adoption of social media has expanded extremely quickly, and the twenty-first century can be regarded as the “boom” era of social networking. Reports from Smart Insights indicate that by February 2019, more than 3.484 billion individuals worldwide were using social media. The report further shows that the global number of social media users is increasing at an annual rate of approximately 9%, a trend expected to persist. Currently, social media users account for about 45% of the world’s population. Reports from 2019 show that children aged 8 to 11 spend an average of 13.5 hours per week online, with 18% actively using social media. Adolescents aged 12 to 15 spend approximately 20.5 hours online weekly, and 69% of them are active on social media platforms. Although children and teenagers form the largest group of Internet users, they generally lack the knowledge required to safeguard their personal data online, making them particularly vulnerable to cybercrimes involving information privacy breaches. In the modern, technology-driven society, data has become one of the most valuable assets for businesses and organizations. Both governments and organizations gather information through various methods, including covert data collection, marketing tools, and search engines such as Google. Data can be obtained from multiple sources and combined using technology to create comprehensive individual profiles. Information shared on social media is easily accessible and highly valuable to both individuals and organizations for purposes such as marketing; as a result, most companies store this data for future use.

3.3 SOCIAL MEDIA

The concept of social networking pre-dates the Internet and mass communication as people are said to be social creatures who when working in groups can achieve results in a value greater than the sun of its parts. The explosive growth in the use of social media over the past decade has made it one of the most popular Internet services in the world, providing new avenues to “see and be seen”. The use of social media has changed the communication landscape resulting in changes in ethical norms and behavior.

The unprecedented level of growth in usage has resulted in the reduction in the use of other media and changes in areas including civic and political engagement, privacy and safety. Alexa, a company that keeps track of traffic on the Web, indicates that as of August, 2019 YouTube.

Facebook and Twitter are among the top four most visited sites with only Google, being the most popular search engine, surpassing these social media sites.

Social media sites can be described as online services that allow users to create profiles which are “public, semi-public” or both. Users may create individual profiles and/or become a part of a group of people with whom they may be acquainted offline. They also provide avenues to create virtual friendships. Through these virtual friendships, people may access details about their contacts ranging from personal background information and interests to location. Social networking sites provide various tools to facilitate communication. These include chat rooms, blogs, private messages, public comments, ways of uploading content external to the site and sharing videos and photographs. Social media is therefore drastically changing the way people communicate and form relationships.

Today social media has proven to be one of the most, if not the most effective medium for the dissemination of information to various audiences. The power of this medium is phenomenal and ranges from its ability to overturn governments (e.g., Moldova), to mobilize protests, assist with getting support for humanitarian aid, organize political campaigns, organize groups to delay the passing of legislation (as in the case with the copyright bill in Canada) to making social media billionaires and millionaires. The enabling nature and the structure of the media that social networking offers provide a wide range of opportunities that were nonexistent before technology. Facebook and YouTube marketers and trainers provide two examples. Today people can interact with and learn from people millions of miles away. The global reach of this medium has removed all former pre-defined boundaries including geographical, social and any other that existed previously. Technological advancements such as Web 2.0 and Web 4.0 which provide the framework for collaboration, have given new meaning to life from various perspectives: political, institutional and social.

3.4 PRIVACY AND SOCIAL MEDIA

Social medial and the information/digital era have “redefined” privacy. In today’s Information Technology - configured societies, where there is continuous monitoring, privacy has taken on a new meaning. Technologies such as closed- circuit cameras (CCTV) are prevalent in public spaces or in some private spaces including our work and home. Personal computers and devices such as our smart phones enabled with Global Positioning System (GPS), Geo locations and Geo maps connected to these devices make privacy as we know it, a thing of the past. Recent reports indicate that some of the largest companies such as Amazon, Microsoft and Facebook as well as various government agencies are collecting information without consent and storing it in databases for future use. It is almost impossible to say privacy exists in this digital world (@nowthisnews).

The open nature of the social networking sites and the avenues they provide for sharing information in a “public or semi-public” space create privacy concerns by their very construct. Information that is inappropriate for some audiences are many times inadvertently made visible to groups other than those intended and can sometimes result in future negative outcomes. One such example is a well-known case recorded in an article entitled “The Web Means the End of Forgetting” that involved a young woman who was denied her college license because of backlash from photographs posted on social media in her private engagement.

Technology has reduced the gap between professional and personal spaces and often results in information exposure to the wrong audience [19]. The reduction in the separation of professional and personal spaces can affect image management especially in a professional setting resulting in the erosion of traditional professional image and impression management. Determining the secondary use of personal information and those who have access to this information should be the prerogative of the individual or group to whom the information belongs. However, engaging in social media activities has removed this control.

Privacy on social networking sites (SNSs) is heavily dependent on the users of these networks because sharing information is the primary way of participating in social communities. Privacy in SNSs is “multifaceted.” Users of these platforms are responsible for protecting their information from third-party data collection and managing their personal profiles.

However, participants are usually more willing to give personal and more private information in SNSs than anywhere else on the Internet. This can be attributed to the feeling of community, comfort and family that these media provide for the most part. Privacy controls are not the priority of social networking site designers and only a small number of the young adolescent users change the default privacy settings of their accounts. This opens the door for breaches especially among the most vulnerable user groups, namely young children, teenagers and the elderly. The nature of social networking sites such as Facebook and Twitter and other social media platforms cause users to re-evaluate and often change their personal privacy standards in order to participate in these social networked communities.

While there are tremendous benefits that can be derived from the effective use of social media there are some unavoidable risks that are involved in its use.
Much attention should therefore be given to what is shared in these forums. Social platforms such as Facebook, Twitter and YouTube are said to be the most effective
media to communicate to Generation Y's (Gen Y's), as teens and young adults are the largest user groups on these platforms. However, according to Boltonet al.
Gen Y's use of social media, if left unabated and unmonitored will have long- term implications for privacy and engagement in civic activities as this continuous use is resulting in changes in behavior and social norms as well as increased levels of cyber-crime.

Today social networks are becoming the platform of choice for hackers and other perpetrators of antisocial behavior. These media offer large volumes of data/ information ranging from an individual's date of birth, place of residence, place of work/business, to information about family and other personal activities. In many cases users unintentionally disclose information that can be both dangerous and inappropriate. Information regarding activities on social media can have far reach- ing negative implications for one's future. A few examples of situations which can, and have been affected are employment, visa acquisition, and college acceptance.
Indiscriminate participation has also resulted in situations such identity theft and bank fraud just to list a few. Protecting privacy in today's networked society can be a great challenge. The digital revolution has indeed distorted our views of privacy, however, there should be clear distinctions between what should be seen by the general public and what should be limited to a selected group. One school of thought is that the only way to have privacy today is not to share information in these networked communities.

However, achieving privacy and control over information flows and disclosure in networked communities is an ongoing process in an environment where contexts change quickly and are sometimes blurred. This requires intentional construction of systems that are designed to mitigate privacy issues.

3.5 ETHICS AND SOCIAL MEDIA

Ethics can be loosely defined as “the right thing to do” or it can be described as the moral philosophy of an individual or group and usually reflects what the individual or group views as good or bad. It is how they classify particular situations by categorizing them as right or wrong. Ethics can also be used to refer to any classification or philosophy of moral values or principles that guides the actions of an individual or group. Ethical values are intended to be guiding principles that if followed, could yield harmonious results and relationships. They seek to give answers to questions such as “How should I be living? How do I achieve the things that are deemed important such as knowledge and happiness or the acquisition of attractive things?” If one chooses happiness, the next question that needs to be answered is “Whose happiness should it be; my own happiness or the happiness of others?” In the domain of social media, some of the ethical questions that must be contemplated and ultimately answered are:

- Can this post be regarded as oversharing?
- Has the information in this post been distorted in anyway?
- What impact will this post have on others?

As previously mentioned, users within the ages 8–15 represent one of the largest social media user groups. These young persons within the 8–15 age range are still learning how to interact with the people around them and are deciding on the moral values that they will embrace. These moral values will help to dictate how they will interact with the world around them. The ethical values that guide our interactions are usually formulated from some moral principle taught to us by someone or a group of individuals including parents, guardians, religious groups, and teachers just to name a few. Many of the Gen Y’s/“Digital Babies” are “newbies” yet are required to determine for themselves the level of responsibility they will display when using the varying social media platforms. This includes considering the impact a post will have on their lives and/or the lives of other persons. They must also understand that when they join a social media network, they are joining a community in which certain behavior must be exhibited. Such responsibility requires a much greater level of maturity than can be expected from them at that age.

It is not uncommon for individuals to post even the smallest details of their lives from the moment they wake up to when they go to bed. They will openly share their location, what they eat at every meal or details about activities typically considered private and personal. They will also share likes and dislikes, thoughts and emotional states and for the most part this has become an accepted norm. Often times however, these shares do not only contain information about the person sharing but information about others as well. Many times, these details are shared on several social media platforms as individuals attempt to ensure that all persons within their social circle are kept updated on their activities. With this openness of sharing risks and challenges arise that are often not considered but can have serious impacts.

The speed and scale with which social media creates information and makes it available almost instantaneously—on a global scale, added to the fact that once something is posted there is really no way of truly removing it, should prompt individuals to think of the possible impact a post can have. Unfortunately, more often than not, posts are made without any thought of the far-reaching impact they can have on the lives of the person posting or others that may be implicated by the post.

Why do people share?

According to Berger and Milkman there are five main reasons why users are compelled to share content online, whether it is every detail or what they deem as highlights of their lives. These are:

- cause related
- personal connection to content
- to feel more involved in the world
- to define who they are
- to inform and entertain

People generally share because they believe that what they are sharing is important. It is hoped that the shared content will be deemed important to others which will ultimately result in more shares, likes and followers.

Content related to a cause

Social media has provided a platform for people to share their thoughts and express concerns with others for what they regard as a worthy cause. Cause related posts are dependent on the interest of the individual.

Some persons might share posts related to causes and issues happening in society. In one example, the parents of a baby with an aggressive form of leukemia, who having been told that their child had only 3 months to live unless a suitable donor for a blood stem cell transplant could be found, made an appeal on social media. The appeal was quickly shared and a suitable donor was soon found. While that was for a good cause, many view social media merely as platforms for freedom of speech because anyone can post any content one creates. People think the expression of their thoughts on social media regarding any topic is permissible. The problem with this is that the content may not be accepted by law or it could violate the rights of someone thus giving rise to ethical questions.

Content with a personal connection

When social media users feel a personal connection to their content, they are more inclined to share the content within their social circles. This is true of informa- tion regarding family and personal activities. Content created by users also invokes a deep feeling of connection as it allows the users to tell their stories and it is natural to want the world or at least friends to know of the achievement. This natural need to share content is not new as humans have been doing this in some form or the other, starting with oral history to the media of the day; social media. Sharing the self-created content gives the user the opportunity of satisfying some fundamental needs of humans to be heard, to matter, to be understood and emancipated. The problem with this however is that in an effort to gratify the fundamental needs, borders are crossed because the content may not be sharable (can this content be shared within the share network?), it may not be share-worthy (who is the audience that would appreciate this content?) or it may be out of context (does the content fit the situation?)

Content that makes them feel more involved in the world

One of the driving factors that pushes users to share content is the need to feel more in tune with the world around them. This desire is many times fueled by jealousy. Many social media users are jealous when their friends' content gets more attention than their own and so there is a lot of pressure to maintain one's
persona in social circles, even when the information is unrealistic, as long as it gets as much attention as possible. Everything has to be perfect. In the case of a photo, for example, there is lighting, camera angle and background to consider.

This need for perfection puts a tremendous amount of pressure on individuals to ensure that posted content is “liked” by friends. They often give very little thought to the amount of their friend’s work that may have gone on behind the scenes to achieve that perfect social post. Social media platforms have provided everyone with a forum to express views, but, as a whole, conversations are more polarized, tribal and hostile. With Facebook for instance, there has been a huge uptick in fake news, altered images, dangerous health claims and cures, and the proliferation of anti-science information. This is very distressing and disturbing because people are too willing to share and to believe without doing their due diligence and fact-checking first.

Content that defines who they are

Establishing one’s individuality in society can be challenging for some persons because not everyone wants to fit in. Some individuals will do all they can to stand out and be noticed. Social media provides the avenue for exposure and many individuals will seek to leverage the media to stand out of the crowd and not just be a fish in the school. Today many young people are currently being brought up in a culture that defines people by their presence on social media where in previous generations, persons were taught to define themselves by their career choices. These lessons would start from childhood by asking children what they wanted to be when they grew up and then rewarding them based on the answers they give. In today’s digital era, however, social media postings and the number of “likes” or “dislikes” they attract, signal what is appealing to others. Therefore, post that are similar to those that receive a large number of likes but which are largely unrealistic are usually made for self-gratification.

Content that informs and entertains

The acquisition of knowledge and skills is a vital part of human survival and social media has made this process much easier. It is not uncommon to hear persons realizing that they need a particular knowledge set that they do not possess say “I need to lean to do this. I’ll just YouTube it.” Learning and adapting to change in as short as possible time is vital in today’s society and social media coupled with the Internet put it all at the finger tips.

Entertainment has the ability to bring people together and is a good way for people to bond. It provides a diversion from the demands of life and fills leisure time with amusement.

Social media is an outlet for fun, pleasurable and enjoyable activities that are so vital to human survival. It is now common place to see persons watching a video, viewing images and reading text that is amusing on any of the available social media platforms. Quite often these videos, images and texts can be both informative and entertaining, but there can be problems however as at times they can cross ethical lines that can lead to conflict.

3.6 ETHICAL CHALLENGES WITH SOCIAL MEDIA USE

The use of modern-day technology has brought several benefits. Social media is no different and chief amongst its benefit is the ability to stay connected easily and quickly as well as build relationships with people with similar interests. As with all technology, there are several challenges that can make the use of social media off putting and unpleasant. Some of these challenges appear to be minor but they can have far reaching effects into the lives of the users of social media and it is therefore advised that care be taken to minimize the challenges associated with the use of social media.

A major challenge with the use of social media is oversharing because when persons share on social media, they tend to share as much as is possible which is often times too much. When persons are out and about doing exciting things, it is natural to want to share this with the world as many users will post a few times a day when they head to lunch, visit a museum, go out to dinner or other places of interest. While this all seems relatively harmless, by using location-based services which pinpoint users with surprising accuracy and in real time, users place themselves in danger of laying out a pattern of movement that can be easily traced. While this seems more like a security or privacy issue it stems from an ethical dilemma “Am I sharing too much?” Oversharing can also lead to damage of user’s reputation especially if the intent is to leverage the platform for business. Photos of drunken behavior, drug use, partying or other inappropriate content can change how you are viewed by others.

Another ethical challenge users of social media often encounter is that they have no way of authenticating content before sharing, which becomes problematic when the content paints people or establishments negatively. Often times content is shared with them by friends, family and colleagues. The unauthenticated content is then re-shared without any thought but sometimes this content may have been maliciously altered so the user unknowingly participates in maligning others.

Even if the content is not altered the fact that the content paints someone or something in a bad light should send off warning bells as to whether or not it is right to share the content which is the underlying principle of ethical behavior.

Conflicting views

Some of the challenges experienced by social media posts are a result of a lack of understanding and sometimes a lack of respect for the varying ethical and moral standpoints of the people involved. We have established that it is typical for persons to post to social media sites without any thought as to how it can affect other persons, but many times these posts are a cause of conflict because of a difference of opinion that may exist and the effect the post may have.

Each individual will have his or her own ethical values and if they differ then this can result in conflict. When an executive of a British company made an Instagram post with some racial connotations before boarding a plane to South Africa it started a frenzy that resulted in the executive's immediate dismissal. Although the executive said it was a joke and there was no prejudice intended, this difference in views as to the implications of the post, resulted in an out of work executive and a company scrambling to maintain its public image.

3.7 IMPACT ON PERSONAL DEVELOPMENT

In this age of sharing, many young person's spend a vast amount of time on social media checking the activities of their "friends" as well as posting on their own activities so their "friends" are aware of what they are up to. Apart from interfering with their academic progress, time spent on these posts at can have long term repercussions. An example is provided by a student of a prominent university who posted pictures of herself having a good time at parties while in school. She was denied employment because of some of her social media posts. While the ethical challenge here is the question of the employee's right to privacy and whether the individual's social media profile should affect their ability to fulfill their responsibilities as an employee, the impact on the individual's long term personal growth is clear.

3.8 CHECK YOUR PROGRESS

Descriptive type questions.

1) List one positive and one negative impact of social media on personal development.
2) How can social media post influence future opportunities such as employment or education?
3) Why is it difficult to completely remove content once it is posted online?
4) Mention one responsible practice users can adopt to protect their privacy on social media.
5) How does social media use influence social norms and behaviour, especially among young users?

Multiple Choice Questions (MCQs)

1. Which of the following best describes social media?

   a) A private communication system used only by organizations

   b) Online services that allow users to create public or semi-public profiles

   c) Software used only for entertainment purposes

   d) A tool designed exclusively for marketing

   Answer: b

2. Why are children and adolescents considered more vulnerable on social media platforms?

   a) They use fewer privacy settings

   b) They spend less time online

   c) They generally lack sufficient knowledge to protect personal data

   d) They do not use social networking sites frequently

   Answer: c

3. Which factor mainly contributes to privacy risks on social networking sites?

   a) High internet speed

   b) Limited user interaction

   c) Users sharing personal information in public or semi-public spaces

   d) Lack of multimedia content

   Answer: c

4. According to ethical principles discussed in this unit, what should a user consider before sharing a post?

   a) The number of likes it may receive

   b) The cost of internet usage

   c) The possible impact the post may have on others

   d) The time of posting

   Answer: c

5. One major ethical challenge associated with social media use is:

   a) Reduced global communication

   b) Oversharing personal information

   c) Limited access to information

   d) Lack of online communities

   Answer: b

UNIT- 4
PREVENTATION AND MEASUREMENT

4.1 OBJECTIVES

After completing this unit, students will be able to:

- Define privacy vs. security and identify 6 major social media threats.
- Apply 10+ practical measures to secure personal accounts.
- Explain Indian laws (IT Act, DPDP Act) and their role in protection.
- Demonstrate safe online behavior through real-world scenarios.
- Design a personal cybersecurity checklist for social media.

4.2 INTRODUCTION

Social media platforms like WhatsApp, Instagram, Facebook, and X have transformed communication, connecting billions worldwide. However, they collect vast personal data, making them prime targets for cybercriminals. This unit explores how to protect your information, major security threats, and advanced measures to safeguard accounts and identity. In India, with 950M+ users (2026), understanding these risks prevents identity theft, fraud (₹10,000 crore annual losses), and harassment.

4.3 HOW TO PROTECT YOUR INFORMATION ON SOCIAL MEDIA

Social media platforms have become an important part of daily life, but they also pose risks to personal information. Protecting information on social media helps prevent identity theft, fraud, cybercrime, and misuse of personal data. Users must be aware and responsible while sharing content online.

1. Use Strong Privacy Settings

Users should customize privacy settings on each social media platform. Profiles should be visible only to trusted friends or connections. Options such as who can view posts, comment, tag, or send messages should be carefully controlled. Regularly reviewing privacy settings is important because platforms often change their policies.

2. Limit the Amount of Personal Information Shared

Avoid sharing sensitive personal details such as phone numbers, home addresses, date of birth, financial details, and identity numbers. Even small pieces of information can be combined by attackers to create a complete personal profile. Users should avoid posting personal documents or confidential images.

3. Create Strong and Unique Passwords

Passwords should be long and difficult to guess. Using a mix of letters, numbers, and symbols makes passwords stronger. Each social media account should have a different password so that if one account is compromised, others remain safe.

4. Enable Two-Factor Authentication (2FA)

Two-factor authentication provides an additional security layer. Even if someone steals the password, they cannot access the account without the verification code. This greatly reduces the chances of hacking and unauthorized access.

5. Be Careful While Accepting Friend Requests

Not all profiles on social media are genuine. Fake accounts are often created to collect personal information or spread scams. Users should verify profiles before accepting friend requests and avoid interacting with unknown users.

6. Avoid Clicking on Suspicious Links and Messages

Cybercriminals often use fake links, messages, or advertisements to trick users into revealing their login details. These phishing attacks may appear to be from trusted sources. Users should always check the sender and avoid clicking unknown or suspicious links.

7. Control Third-Party App Access

Many apps request permission to access social media accounts. Users should carefully read permission requests and deny unnecessary access. Apps that are no longer in use should be removed to reduce the risk of data misuse.

8. Think Before Posting Content

Once information is posted online, it can be copied, downloaded, or shared by others. Even deleted content may remain stored on servers. Users should think carefully before posting personal photos, opinions, or private information.

9. Turn Off Location Sharing

Sharing real-time location can be dangerous. Location settings should be disabled unless necessary. Posting travel updates after returning home is safer than sharing live locations.

10. Educate Yourself About Online Scams

Users should stay informed about new online scams, fake giveaways, and fraud techniques. Awareness helps users identify threats early and avoid falling victim to cybercrime.

4.4 SECURITY IN SOCIAL MEDIA

Social media security refers to the practices and technologies used to protect user accounts, personal data, and digital identity from unauthorized access, cyberattacks, and misuse. With the increasing number of users on social networking platforms, security has become a major concern for individuals, organizations, and governments.

Importance of Social Media Security

- Protects personal and sensitive information from hackers
- Prevents identity theft and online impersonation
- Ensures safe communication and interaction
- Reduces the risk of financial loss and fraud
- Protects users from cyberbullying and harassment
- Maintains trust in digital platforms

Major Security Threats on Social Media

1. Hacking

Hackers gain unauthorized access to accounts by guessing passwords, using malware, or exploiting weak security settings.

2. Phishing Attacks

Fake messages or emails appear to be from trusted sources and trick users into sharing login details or personal information.

3. Malware and Spyware

Malicious software may be spread through links, ads, or infected files, allowing attackers to monitor user activity or steal data.

4. Identity Theft

Cybercriminals steal personal information and create fake profiles to impersonate users for illegal activities.

5. Account Hijacking

Attackers take control of social media accounts and use them to spread scams, spam, or harmful content.

6. Data Breaches

Large amounts of user data may be leaked due to weak security systems or cyberattacks on platforms.

4.5 ADVANCED SECURITY MEASURES ON SOCIAL MEDIA

Use Strong Authentication Methods: *In addition to passwords, users should enable two-factor or multi-factor authentication. This ensures that access is granted only after verifying identity through multiple steps.*

Regularly Update Passwords: *Passwords should be changed periodically. Old or compromised passwords should never be reused.*

Enable Login Alerts: Most platforms allow users to receive alerts when a login attempt occurs from a new device or location. This helps detect unauthorized access quickly.

Secure Email Linked to Social Media: *Email accounts connected to social media must also be secured with strong passwords and two-factor authentication, as they are often used for password recovery.*

Avoid Third-Party Login Options: *Logging into apps or websites using social media accounts may expose data. Users should minimize such connections.*

Review Active Sessions: Users should regularly check and log out of devices where the account is currently logged in, especially if a device is lost or shared.

Device and Network Security

Install Antivirus and Security Software: *Security software helps detect and remove malware, spyware, and harmful applications.*

Use Firewalls: Firewalls help block unauthorized access to devices and networks.

Encrypt Devices: Using device encryption protects stored data in case the device is stolen or lost.

Use Secure Browsers: Updated and secure browsers reduce exposure to malicious websites and attacks.

Behavioral Security Practices

Be Cautious with Online Interactions: Users should avoid sharing personal details in comments, chats, or public posts.

Do Not Share One-Time Passwords (OTPs): *OTPs and verification codes should never be shared with anyone, even if they claim to be from customer support.*

Avoid Using Social Media on Public Computers: *Public systems may have keyloggers or spyware installed.*

Think Before Responding to Messages: Messages creating urgency, fear, or excitement are often scams.

Platform-Level Security Features

Reporting and Blocking Tools: Users should actively report suspicious, abusive, or fake accounts to the platform.

Content Moderation Systems: Platforms use automated tools and human moderators to detect harmful content and suspicious behavior.

Data Encryption by Platforms: Most social media platforms use encryption to protect user data during transmission.

Role of User Awareness in Security

User awareness plays a crucial role in social media security. Even the strongest security systems can fail if users are careless. Regular digital literacy programs and cybersecurity awareness help users recognize threats and adopt safe practices.

4.4 CHECK YOUR PROGRESS

Descriptive Questions

1. Explain the importance of protecting personal information on social media.
2. What are strong privacy settings? Explain how they help users stay safe on social media.
3. Describe any four major security threats on social media.
4. Explain the role of user awareness in ensuring social media security.
5. What are advanced security measures on social media? Explain any five.

Multiple Choice Questions (MCQs)

(Easy & from the same content)

1. Which of the following helps prevent unauthorized access to social media accounts?

   a) Weak passwords

   b) Two-factor authentication

   c) Public profiles

   d) Location sharing

   Answer: b

2. Sharing real-time location on social media can lead to:

   a) Better networking

   b) Increased privacy

   c) Security risks

   d) Faster communication

   Answer: c

3. Phishing attacks mainly aim to:

   a) Improve security

   b) Steal login details

   c) Block accounts

   d) Delete data

   Answer: b

4. Which of the following is an example of a major social media security threat?

   a) Encryption

   b) Antivirus software

   c) Account hijacking

d) Privacy settings

Answer: c

5. Oversharing on social media can lead to:

a) Improved safety

b) Identity theft and privacy risks

c) Stronger passwords

d) Better content quality

Answer: b

BLOCK -2
PRIVACY AND SECURITY

BLOCK -2

UNIT – 5

Privacy in Social Media

Unit Structure

5.1 OBJECTIVE

After this unit, students will be able to:

- Define privacy and explain its 7 dimensions with Indian examples.
- Distinguish digital footprint types and manage online identity risks.
- Analyze data collection methods, profiling uses, and 6 ethical concerns.
- Identify 7 social media privacy risks and apply 15+ preventive measures.
- Apply legal frameworks (IT Act, DPDP) and security practices for safe usage.

5.2 INTRODUCTION

In the digital age, people use the internet for communication, education, banking, shopping, entertainment, and social networking. While these technologies provide convenience and connectivity, they also raise serious concerns about **privacy**. Personal information such as name, location, photos, preferences, and online behaviour is constantly collected, stored, and shared. Understanding digital privacy is essential to protect individuals from misuse of personal data, identity theft, surveillance, and cybercrime.

5.2 MEANING AND DIMENSIONS OF PRIVACY

Meaning of Privacy

Privacy refers to an individual's right to control their personal information and decide how, when, and to what extent it is shared with others. It encompasses not just data but also personal autonomy, protecting against unwanted intrusion into one's life, body, or decisions. This right is foundational in legal frameworks like India's Article 21 (right to life and personal liberty) and global standards such as the GDPR in Europe.

Dimensions of Privacy

- **Information Privacy**: Protection of personal data such as name, phone number, Aadhaar number, financial details, and medical records. This dimension focuses on preventing unauthorized collection, storage, or sharing of identifiable information, often safeguarded by laws like India's Digital Personal Data Protection Act (DPDP), 2023.

- **Communication Privacy**: Privacy of emails, messages, phone calls, and online chats. It ensures confidentiality in interpersonal exchanges, shielding against eavesdropping, data interception, or compelled disclosure, as protected under telecom regulations and encryption standards.
- **Physical Privacy:** Protection from physical surveillance, such as CCTV misuse or unauthorized tracking. This includes safeguards against unwarranted searches, home intrusions, or biometric monitoring without consent, balancing public safety with individual rights.
- **Decisional Privacy:** Freedom to make personal choices without external interference (e.g., beliefs, lifestyle choices). This dimension empowers individuals to form intimate relationships, religious convictions, reproductive decisions, and family matters privately, free from state or societal coercion.
- **Additional aspects include:**

Bodily Privacy: Autonomy over one's body, such as consent for medical procedures, vaccinations, or gender-affirming care. For instance, forcing medical treatments without informed consent violates this, as seen in debates over mandatory health policies.

Relational Privacy: The right to choose associations, like marriage, friendships, or sexual orientation, without judgment or penalty. India's Supreme Court recognition of privacy.

Associational Privacy: Freedom to join groups, unions, or political parties privately, protecting against surveillance of memberships that could lead to discrimination.

Locational Privacy: Control over tracking one's movements via GPS or apps, preventing inferences about habits or routines.

These dimensions often overlap - for example, sharing location data (information privacy) can reveal lifestyle choices (decisional privacy). In India, evolving jurisprudence like the Puttaswamy judgment (2017) affirms privacy as intrinsic to dignity.

5.3 DIGITAL FOOTPRINT AND ONLINE IDENTITY

Digital Footprint

A digital footprint is the trail of data created by users while using the internet. It persists across platforms and can influence opportunities like jobs or loans, often outlasting the user's control. In India, with over 900 million internet users (as of 2025), managing this footprint is crucial under laws like the DPDP Act.

Types of Digital Footprint

Active Digital Footprint: Data shared intentionally (posts, comments, form submissions). Examples include uploading photos on Instagram or filling out e-commerce profiles.

Passive Digital Footprint: Data collected without direct user awareness (cookies, tracking, and browsing history). This includes IP logs, device fingerprints, and geolocation from apps, often used for targeted ads.

Online Identity

Online identity is how a person is represented on the internet, including social media profiles, email accounts, usernames, and avatars. It shapes perceptions by others and can be fragmented across platforms or deliberately curated (e.g., via pseudonyms). Unlike real-world identity, it's malleable but vulnerable to hacking or misrepresentation.

Key components and aspects include:

- **Social Media Profiles:** Curated personas on platforms like Facebook, Instagram, or X (formerly Twitter), revealing interests, networks, and timelines.
- **Email Accounts and Digital Signatures:** Gateways to services, often linked to verified identities via two-factor authentication.
- **Usernames and Avatars:** Digital handles and visuals that signal personality, anonymity, or branding (e.g., gamer tags on Discord).
- **Online Behaviour and Reputation:** Patterns like posting frequency, engagement style, or review history that build a "reputation score." Tools like Google searches or Klout scores quantify this.
- **Biometric and Verified Identities:** Linked accounts via Aadhaar, UPI handles, or facial recognition on apps like WhatsApp.
- **Shadow Profiles:** Invisible data aggregates (e.g., Facebook's inferred profiles from friends' data) that exist without user knowledge.

Risks and Management

Online identities can lead to doxxing, identity theft, or biased algorithms (e.g., denied loans due to old posts). To manage: Use privacy settings, VPNs, delete old accounts via tools like JustDeleteMe, and monitor with services like Have I Been Pwned? Example: In 2023, a viral LinkedIn post cost a job seeker an offer due to mismatched online behaviour. These concepts intersect with privacy - your digital footprint forms the basis of your online identity, amplifying risks in India's growing digital economy.

5.4 DATA COLLECTION AND USER PROFILLING

Data Collection

Organizations collect user data through various digital touchpoints to fuel business models and services. This data forms the backbone of the modern internet economy.

Methods include:

- Cookies and trackers (e.g., third-party pixels from Google Analytics).
- Online forms (e.g., sign-ups capturing emails and preferences).
- Social media interactions (e.g., likes, shares on Meta platforms).
- Mobile apps and GPS (e.g., location pings from Uber or Swiggy).

User Profiling

User profiling is the process of analyzing collected data to understand user behavior, interests, preferences, and habits. It uses AI and machine learning to create detailed "user personas," often scoring users on traits like purchase likelihood or political leanings.

Uses of User Profiling

Targeted advertising (e.g., showing shoe ads after browsing sneakers).

Personalized content (e.g., Netflix tailoring watchlists).

Recommendation systems (e.g., Amazon's "customers also bought").

Market research (e.g., predicting trends from aggregated habits).

Concerns

While beneficial, user profiling raises serious ethical and legal issues, often prioritizing profits over rights.

Expanded concerns include:

Loss of Privacy: Constant surveillance erodes anonymity; passive data like browsing history reveals sensitive details without consent. Example: Cambridge Analytica scandal (2018) exposed how Facebook data profiled 87 million users for elections.

Manipulation of User Behavior: Algorithms nudge choices via filter bubbles or addictive feeds, exploiting psychological biases (e.g., TikTok's "For You" page keeping users scrolling).

Discrimination: Biased profiles perpetuate inequality; facial recognition misidentifies darker skin tones, or credit scoring disadvantages low-income groups. In India, this affects Aadhaar-linked services.

Data Misuse and Breaches: Hacked profiles lead to identity theft or blackmail; sold data fuels spam or fraud. 2024's massive AT&T breach exposed 73 million profiles.

Lack of Transparency and Consent: "Dark patterns" trick users into sharing (e.g., pre-checked boxes); profiling happens invisibly via cross-site tracking.

Surveillance Capitalism: Companies like Google monetize predictions of behavior, commodifying personal lives.

Legal and Mitigation Measures
India's DPDP Act (2023) mandates consent, data minimization, and rights like erasure. Globally, GDPR fines (e.g., €1.2B on Meta in 2023) enforce accountability. Users can opt for privacy-focused browsers (e.g., DuckDuckGo), ad blockers, or tools like Privacy Badger. Example: Apple's App Tracking Transparency (2021) lets users block profiling, slashing ad revenues.
These practices highlight the tension between innovation and individual control in a data-driven world.
Here's an expanded version of your outline on "Privacy Risks in Social Media." I've fleshed out each risk with explanations, examples, and impacts, then added a detailed "Preventive Measures" section with practical steps, stats, and an illustrative example for completeness.

5.6 Privacy Risks in Social Media

Social media platforms pose several privacy risks due to their vast data collection, public sharing defaults, and interconnected ecosystems. With India's 500+ million users (2025 stats), these risks amplify in diverse contexts like family networks or political discourse.

Key Privacy Risks

Oversharing Personal Information: Users post details like addresses, routines, or family photos impulsively, enabling strangers to piece together profiles.

Impact: Leads to burglary (e.g., "empty house" posts during vacations).

Identity Theft: Stolen credentials or profile data allow impersonation for scams or fraud. Example: Phishing via fake friend requests.

Cyberstalking and Harassment: Trackers exploit posts to monitor locations or harass (e.g., doxxing on X/Twitter). India's 2024 NCRB data shows rising cyberstalking cases.

Data Breaches: Hacks expose millions of records; 2023 Meta breach leaked 6TB of user data.

Facial Recognition Misuse: Auto-tagging scans faces without consent, feeding surveillance databases (e.g., Clearview AI controversies).

Third-Party App Access: "Log in with Facebook" grants apps broad data permissions, often forgotten and revocable only manually.

Location Tracking: Check-ins or geotags reveal real-time movements, risking safety (e.g., stalkers using Instagram Stories).

Preventive Measures Protect yourself with proactive habits and tools:

Privacy Settings: Set profiles to private, limit post visibility (e.g., "Friends only" on Facebook), and disable location services. Review monthly.

Minimize Sharing: Avoid posting sensitive info; use Stories that auto-delete instead of permanent feeds. Think "STRANGER test"—would you share with a stranger?

Strong Authentication: Enable 2FA, unique passwords via managers like LastPass, and biometric locks.

App Permissions: Revoke third-party access regularly (e.g., Facebook's "Apps and Websites" section); deny unnecessary permissions.

Tools and Features: Use VPNs (e.g., ExpressVPN), ad blockers, and platform tools like Instagram's "Close Friends." Opt out of facial recognition where possible.

Awareness and Reporting: Educate on phishing; report violations promptly (e.g., Twitter's harassment tools). In India, use cybercrime.gov.in for complaints.

Digital Hygiene: Regularly delete old posts/accounts; use ephemeral apps like Signal for sensitive chats.

5.7 Preventive Measures

Protect your privacy through layered habits, tools, and awareness. These steps minimize risks like data breaches, stalking, and profiling across apps and platforms.

Core Practices

Strong Privacy Settings: Customize platform defaults—set social media to private, limit audience (e.g., Facebook "Friends only"), and disable public searchability. Review quarterly.

Two-Factor Authentication (2FA): Add a second verification layer (e.g., app like Google Authenticator or SMS); enables on Gmail, Instagram. Reduces account hacks by 99% (Google stats).

Avoid Sharing Sensitive Data: Skip posting addresses, Aadhaar, financials, or routines; use vague terms like "out with friends" instead of locations.

Regular Password Updates: Change every 3-6 months; use 12+ character passphrases (e.g., "BlueHorseBatteryStaple") via managers like Bitwarden or 1Password. Avoid reuse.

Advanced Strategies

Awareness of Fake Profiles: Verify via reverse image search (Google Lens), mutual connections, or blue ticks. Report/block suspicious accounts immediately.

Permission Management: Audit app permissions (e.g., revoke camera/mic access); use "Log in with Google" sparingly and review linked apps.

Data Minimization Tools: Employ ad blockers (uBlock Origin), tracker blockers (Privacy Badger), and VPNs (ProtonVPN) to cut passive tracking.

Device and Software Hygiene: Keep OS/apps updated, use antivirus (e.g., Malwarebytes), and enable full-disk encryption (BitLocker on Windows).

Digital Footprint Cleanup: Delete old posts/accounts with tools like JustDeleteMe; request data deletion under DPDP Act or GDPR. Monitor breaches via Have I Been Pwned.

Education and Backup: Stay informed via resources like India's Cyber Swachhta Kendra; back up data securely before resets.

Illustrative Example: A user hit by a 2025 LinkedIn phishing scam enabled 2FA, switched to a password manager, and scanned for fakes—preventing further breaches and recovering their profile safely.

Consistency is key: Treat privacy like hygiene—daily habits yield long-term protection.

5.8 Check Your Progress

1. Define privacy and explain its major dimensions with suitable Indian examples.
2. What is a digital footprint? Explain its types and discuss how it affects online identity.
3. Explain the concept of online identity and discuss the risks associated with managing online identity.
4. Describe the methods of data collection and explain how user profiling is carried out by organizations.

5. Discuss the ethical concerns related to data collection and user profiling with relevant examples.

6. Explain the major privacy risks in social media and describe the preventive measures users can take to protect their privacy.

UNIT : 6

Social Media and Privacy

Unit Structure

6.0 Objective

After completing this unit, students will be able to:

- Understand how social media has changed communication and affected personal privacy.

- Explain the privacy paradox and factors influencing online self-disclosure.

- Analyze social media privacy using the boundary regulation perspective.

- Identify and explain different types of privacy boundaries on social media.

- Understand individual differences in privacy attitudes and their impact on platform design.

- Evaluate privacy challenges, social disenfranchisement, and guidelines for designing privacy-sensitive social media platforms.

6.1 Introduction

The way people communicate with one another in the twenty-first century has evolved rapidly. In the 1990s, if someone wanted to share a “how-to” video tutorial within their social networks, the dissemination optionswould be limited (e.g., email, floppy disk, or possibly a writeable compact disc). Now, social media platforms, such as TikTok, provide professional grade video editing and sharing capabilities that give users the potential to both create and disseminate such content to thousands of viewers within a matter of minutes. As such, social media has steadily become an integral component for how people capture aspects of their physical lives and share them with others. Social media platforms have gradually altered the way many people live, learn, and maintain relationships with others.

6.2 Privacy Paradox

While researchers have investigated these various privacy attitudes, perceptions, and behaviors, the privacy paradox (where behavior does not match with stated privacy concerns) has been especially salient on social media. As a result, much research focuses on understanding the decision-making process behind selfdisclosure. Scholars that view disclosure as a result of weighing the costs and the benefits of disclosing information use the term “privacy calculus” to characterize this process. Other research draws on the theory of bounded rationality to explain how people’s actions are not fully rational. They are often guided by heuristic cues which do not necessarily lead them to make the best privacy decisions. Indeed, a large body of literature has tried to dispel or explain the privacy paradox.

6.3 Reconceptualizing Social Media Privacy as Boundary Regulation

By reconceptualizing privacy in social media as a boundary regulation, we can see that the seeming paradox in privacy is actually a balance between being too open or disclosing too much and being too inaccessible or disclosing too little. The latter can result in social isolation which is privacy regulation gone wrong.

In the context of social media, there are five different types of privacy boundaries that should be considered. People use various methods of coping with privacy violations, many not tied to disclosing less information. Drawing from Altman’s theories of privacy in the offline world, Palen and Dourish describe how, just like in the real world, social media privacy is a boundary regulation process along various dimensions besides just disclosure. Privacy can also involve regulating interactional boundaries with friends or followers online and the level of accessibility one desires to those people. For example, if a Facebook user wants to limit the people that can post on their wall, they can exclude certain people. Research has identified other threats to interpersonal boundary regulation that arise out of the unique nature of social media. First, as mentioned previously, the threat to spatial boundaries occurs because our audiences are obscured so that we no longer have a good sense of whom we may be interacting with. Second, temporal boundaries are blurred because any interaction may now occur asynchronously at some time in the future due to the virtual persistence of data. Third, multiple interpersonal spaces are merging and overlapping in a way that has caused a “steady erosion of clearly situated action”. Since each space may have different and, at times, mutually exclusive behavioral requirements, acting accordingly within those spaces has become more of a challenge to manage context collapses. Along with these problems, a major interpersonal boundary regulation challenge is that social media environments often take control of boundary regulation away from the end users. For instance, Facebook's popular "Timeline" automatically (based on an obscure algorithm) broadcasts an individual's content and interactions to all of his or her friends. Thus, Facebook users struggle to keep up to date on how to manage interactions within these spaces as Facebook, not the end user, controls what is shared with whom.

6.4 Boundary Regulation on Social Media

One conceptualization of privacy that has become popular in the recent literature is viewing privacy on social media as a form of interpersonal boundary regulation. These scholars have characterized privacy as finding the optimal or appropriate level of privacy rather than the act of withholding self-disclosures. That is, it is just as important to avoid over disclosing as it is to avoid under disclosing. Therefore, disclosure is considered a boundary that must be regulated so that it is not too much or too little. Petronio's communication privacy management (CPM) theory emphasizes how disclosing information is vital for building relationships, creating closeness, and creating intimacy. Thus, social isolation and loneliness resulting from under disclosure can be outcomes of privacy regulation gone wrong just as much as social crowding can be an issue. Similarly, the framework of contextual integrity explains that context-relative informational norms define privacy expectations and appropriate information flows and so a disclosure in one context (such as your doctor asking you for your personal medical details) may be perfectly appropriate in that context but not in another (such as your employer asking you for your personal medical details). Here it is not just about an information disclosure boundary but about a relationship boundary where the appropriate disclosure depends on the relationship between the discloser and the recipient. Drawing on Altman's theory of boundary regulation, Wisniewski et al. created a useful taxonomy detailing the various types of privacy boundaries that are relevant for managing one's privacy on social media. They identified five distinct privacy boundaries relevant to social media:

1. **Relationship:** This involves regulating who is in one's social network as well as appropriate interactions for each relationship type.

2. **Network:** This consists of regulating access to one's social connections as well as interactions between those connections.

3. Territorial: This has to do with regulating what content comes in for personal consumption and what is available in interactional spaces.

4. Disclosure: The literature commonly focuses on this aspect which consists of regulating what personal and co-owned information is disclosed to one's social network.

5. Interactional: This applies to regulating potential interaction with those within and outside of one's social network.

Of these boundary types, Wisniewski et al. emphasize the most important is maintaining relationship boundaries between people. Similarly, Child and Petronio note that "one of the most obvious issues emerging from the impact of social network site use is the challenge of drawing boundary lines that denote where relationships begin and end". Making sure that social media facilitates behavior appropriate to each of the user's relationships is a major challenge. Each of these interpersonal boundaries can be further classified into regulation of more fine-grained dimensions. Self- and Confidant Disclosures The information disclosure concerns described in the previous "Privacy Challenges" section are the focus of privacy around disclosure boundaries. Posting norms on social media platforms often encourage the disclosure of one's personal information (e.g., age, sexual orientation, location, personal images). Disclosing such information can leave one open to financial, personal, and professional risks such as identity theft. However, there are motivations for disclosing personal information. For example, research suggests that posting behaviors on social media platforms have a significant relationship with a desire for positive self-presentation. Privacy management is necessary for balancing the benefits of disclosure and its associated risks.

6.5 Addressing Privacy Challenges

Rather than just measuring privacy concerns, researchers and designers should focus on understanding attitudes towards boundary regulation. Validated tools for measuring boundary preservation concern and boundary enhancement expectations are provided in this chapter.

Privacy features need to be designed to account for individual differences in how they are perceived and used. While some feel features like untag, unfriend, and delete are useful, others are worried about how using such features will impact their relationships.

Unaddressed privacy concerns can serve as a barrier to using social media. It is crucial to design for not only functional privacy concerns (e.g., being overloaded by information, guarding from inappropriate data access) but social privacy concerns as well (e.g., unwelcome interactions, pressures surrounding appropriate self-presentation). This section describes how to better identify privacy concerns by measuring them from a boundary regulation perspective.We also emphasize the importance of individual differences when designing privacy features. Finally, we elaborate on a crucial set of social privacy issues that we feel are a priority to address. While many social media users may feel these types of social pressures to some degree, these problems have pushed some of society's most vulnerable to complete abandonment of social media despite their desire for social connection. We call on social media designers and researchers to focus on these problems which are a side effect of the technologies we have created.

6.6 Understanding People and Their Privacy Concerns

Understanding social media privacy as a boundary regulation allows us to better conceptualize people's attitudes and behaviors. It helps us anticipate their concerns and balance between too little or too much privacy. However, many existing tools for measuring privacy come from the information privacy perspective and focus on data collection by organizations, errors, secondary use, or technical control of data. In detailing the various types of privacy boundaries that are relevant for managing one's privacy on social media, Wisniewski et al. emphasized that the most important is maintaining relationship boundaries between people. similarly found that concerns about damaging relationship boundaries are actually at the root of low-level privacy concerns such as worrying about who sees what, being too accessible, or being bothered or bothering others by sharing too much information. For instance, a typically cited privacy concern such as being worried about a stranger knowing one's current location turns out to be a privacy concern only if an individual expects that a stranger might violate.

6.7 Measuring Privacy Concerns

Boundary regulation plays a key role in maintaining the right level of privacy on social media, but how do we evaluate whether a platform is adequately supporting it? A popular scale for testing users' awareness of secondary access is the Internet Users' Information Privacy Concerns (IUIPC) scale, which measures their perceptions of collection, control, and awareness of user data. An important finding is that users "want to know and have control over their information stored in marketers' databases." This indicates that social media should be designed such that people know where their data goes. However, throughout this chapter, it is evident that research on social media privacy has found concerns about social privacy more salient. In fact, the focus on relationship boundaries is a key privacy boundary to consider and measure in evaluating privacy concerns. Thus, having a scale to measure relationship boundary regulation would allow researchers and designers to better evaluate social media privacy.

For instance, Facebook, one of the most widely used platforms, was shown to both invoke high levels of concern as well as high levels of enhancement expectation. However, note that high frequency of use does not necessarily mean high levels of engagement (e.g., posting, commenting) or that users do not employ suboptimal workarounds (e.g., being vague in their posts). On the other hand, Twitter has a higher level of concerns compared to perceived enhancement and, accordingly, lower levels of usage.

6.8 Designing Privacy Features

When designing for privacy features, a crucial aspect to consider is individual differences. Privacy is not one-size-fits-all: there are many variations in how people feel, what they expect, and how they behave. Because social media connects individuals with diverse needs and expectations, and from a myriad of contexts, a necessity in addressing social media privacy is understanding individual differences in privacy attitudes and behaviors. Many individual differences have been identified that shape privacy needs and preferences and behaviors. Scholars have established that privacy as a construct is not limited to informational privacy (i.e., understanding the flow of data) but also includes social privacy concerns that may be more interactional (e.g., accessibility) or psychological in nature (e.g., self-presentation). Thus, a host of attitudes and experiences could shape an individual's view on what it means to have privacy online. For example, people's preferences for privacy tools could be heavily influenced by the type of data being shared or the recipient of that data. Likewise, prior experiences (negative or positive) could shape how people interact online which could affect disclosure. Context and relevance have also been found to significantly influence privacy behavior online. Drawing from the contextual integrity framework, many researchers argue that when people perceive data collection to be reasonable or appropriate, they are more likely to share information. On the other hand, research has shown that when faced with uncomfortable scenarios, people employ privacy protective behaviors such as nondisclosure or falsifying information. Research has also pointed to personal characteristics that could shape digital privacy behavior such as personality, culture, gender, age, and social norms.

While identifying concerns about damaging one's relationships is important to measure, understanding the individual differences that can lead someone to be concerned can provide insight into addressing these concerns. For instance, through a series of investigations, Page et al. uncovered a communication style that predicts concerns about preserving relationship boundaries on many different social media platforms. This communication style is characterized by wanting to put information out there so that the individual does not need to proactively inform others. Those who prefer an FYI (For Your Information) communication style are less concerned about relationship boundary preservation and, as a result, exhibit higher levels of engagement, interactions, and use of social media than low FYI communicators. For example, the survey items that capture an FYI communication style preference for location-sharing social media are: "I want the people I know to be aware of my location, without having to bother to tell them," "I would prefer to make my location available to the people I know, so that they can see it whenever they need it," and "The people I know should be able to get my location whenever they feel they need it." Each item is administered with a 7-point Likert scale (Disagree strongly, Disagree moderately, Disagree slightly, Neutral, Agree slightly, Agree moderately, Agree strongly). For other social media platforms, the information type is adjusted (i.e., "what I'm up to" instead of "my location").

Consequently, this raises concern over implications for non-FYI communicators since the design of major social media platforms is catered to FYI communicators. Drawing on this insight, Page demonstrated how considering the user's communication style when designing location-sharing socialmedia interfaces can alleviate boundary preservation concerns [129]. Certain design choices such as choosing a request-based location-sharing interaction can lower concerns fornon-FYI communicators, while continuous location-sharing and check-in type interactions that are typical in social media may be fine for FYI communicators.

This demonstrates that researchers should consider in the design of social media individual differences that affect privacy attitudes. Another individual difference in attitudes towards privacy features is a user's apprehension that using common features such as untag, delete, or unfriend/unfollow can act as a hindrance in their relationships with others. Page et al. identified that while many use privacy features and perceive them as a tool useful for protecting their privacy, there are also many who are concerned about how using privacy features could hurt their relationships with others (e.g., being worried about offending others by untagging or unfriending). Instead, those individuals would use alternative privacy management tactics such as vaguebooking (not sharing specific details and using vague posts). Designers need to be aware that privacy features also need to be catered to individual variations in attitudes as well or else they may be ineffective and unused by certain segments of the user population.

6.9 Privacy Concerns and Social Disenfranchisement

A significant amount of research within the domain of social media nonuse has been focused on functional barriers that hinder adoption. In many cases, nonuse is traced to a lack of access (e.g., limited access to technology, financial resources, or the Internet). However, the push against adoption and subsequent usage can be voluntary due to functional privacy concerns such as concerns about data breaches, information overload, or annoying posts [120]. Several social media companies have also implemented features such as time limits to help users counter overuse.

Likewise, it is equally important to consider social barriers that prevent social media engagement for people who really could use the social connection. Sharing about distressing experiences can be beneficial and reduce stigma, improve connection and interpersonal relationships with one’s network, and enhance well-being However, Page et al. identified a class of barriers that highlight social privacy concerns rooted in social anxiety or concerns about being overly influenced by others on social media. This is in contrast to the prior school of thought that focused primarily on functional motivations as barriers that influence nonuse. They point out that many who are already vulnerable avoid social media due to social barriers such as online harassment or paralysis over making decisions pertaining to online social interactions. Yet, they are also the ones who could benefit greatly from social connection and who end up losing touch with friends and social support by being off social media. They term this lose-lose situation of negative social consequences that arise when using social media as well as consequences from not using it, social disenfranchisement. They call on designers to address such social barriers and to realize that in designing the user experience to connect users so well, they are implicitly designing the nonuser experience of being left out. Given that social media usage may not always be a viable option, designers should design to alleviate the negative consequences of nonuse.

6.10 Guidelines for Designing Privacy-Sensitive Social Media

Now that you have learned about various privacy problems related to social media use, how do you apply that to designing or studying social media? Here are some practical guidelines.

Identifying Privacy Attitudes Measuring privacy attitudes is a tricky task. Using existing informational privacy scales, users often say they are concerned, but this does not end up matching their actual behavior. By approaching it from a boundary regulation perspective, it will be easier to identify the proper balance between sharing too much and sharing too little. The survey items described in this chapter offer a way to measure concerns about boundary regulation as well as positive expectations. Considering both are key to more accurately predicting user behaviors.

Understanding Your Target Population Some key characteristics are described in this chapter. Identifying these in your target population can help you be aware of individual differences that might affect privacy preferences on social media. When you are measuring privacy concerns, matching the preferences of your audience makes it more likely that they will have a good user experience. Pay particular attention to traits that have been identified as being related to usage and adoption of social media platforms, such as the FYI communication style which can be measured using the survey items provided in this chapter.

Evaluating Privacy Features Focus on understandingwhether users perceive your privacy features as useful or perhaps as posing a relational hindrance. The survey items provided in this chapter can help you do so. When anticipating privacy needs of your social media users, make sure you identify features that may impact boundary regulation both positively and negatively. You can compare attitudes between the existing feature and the newer version of the feature that will/has been deployed. You can also correlate attitudes towards privacy features with individual characteristics – some subpopulation of users may see privacy features as useful, while others may consider them a relational hindrance.

6.11 Check Your Progress

1. Explain how social media has transformed communication in the twenty-first century and discuss its impact on privacy.
2. What is the Privacy Paradox? Explain it with reference to privacy calculus and bounded rationality.

UNIT - 7

Privacy-Enhancing Technologies

Unit Structure

7.0 Objective

After completing this unit, students will be able to:

- Understand the concept and importance of privacy-enhancing technologies.
- Explain how secure messaging and end-to-end encryption protect communication.
- Identify privacy threats such as eavesdropping, MITM attacks, and data breaches.
- Describe the role of HTTPS and TLS in securing data transmission.
- Understand two-factor authentication and its importance in account security.
- Apply safe online practices to protect privacy and digital identity.

7.1 Introduction

An increasing amount of sensitive information is being communicated, stored, and shared online. Unauthorized access to this information can lead to serious privacy violations. This chapter focuses on some privacy-enhancing technologies (PETS) that prevent unauthorized access to sensitive information.

The need for effective privacy-enhancing technologies has never been greater. The Snowden revelations in 2013 exposed a broad array of government surveillance programs and ignited renewed interest in privacy-preserving technologies that prevent eavesdropping. The steady stream of data breaches underscores the risks of trusting third parties with sensitive information and the importance of robust defenses against unauthorized account access. Along with the risk of sensitive information disclosure, the rise of online social networks and other data-sharing cloud services presents increasing opportunities for privacy violations.

This chapter discusses several technologies that the usable security research community has analyzed and identifies issues, recommendations, and future research irections. For example, privacy-enhancing technologies protect sensitive information during transmission (HTTPS) and storage at untrusted third parties (end-to-end encryption in secure messaging and secure email). Technologies can also keep sensitive conversations private so that the fact that two parties are even communicating is not made public (Tor). Usable security researchers explore the human-computer interaction aspects of PETS, an important socio-technical element beyond the formal security guarantees established by a security analysis. A security technology that is not usable can lead to reduced security or no security at all.

7.2 Secure Messaging

Instant messaging (IM) applications provide an online chat capability that allows users to communicate in real time.Without end-to-end encryption, the conversation is not private. Early IM applications did not provide any encryption, allowing eavesdropping by the service provider or anyone with access to the network during transmission. For instance, other users on a wireless network with the proper software could easily view the chat messages.

IM applications typically rely on a centralized server to relay messages between the users. If each user connects to the server using HTTPS, no network eavesdroppers can read the messages. However, the service provider has access to the entire chat conversation when the server relays or stores the plaintext messages.

A significant post-Snowden development was the creation of the Signal Protocol by Moxie Marlinspike and Trevor Perrin. The protocol provides end-to-end encryption and is available inWhatsApp, the Signal app by OpenWhisper Systems, and Facebook Messenger Secret Conversations. Together, these applications serve over a billion users. Moxie and Trevor received the 2017 Levchin Prize for Real- World Cryptography for the development and widespread deployment of the Signal Protocol.

The widespread adoption and use of the Signal Protocol may represent the argest, most rapid adoption of end-to-end encryption in history. Interestingly, privacy was not a driving motivation for users to adopt these systems. Instead, adoption was based on the natural spread of messaging applications so that friends could communicate with their friends. The privacy benefits of encrypted conversations are a side benefit that did not drive adoption. Nonetheless, the result is that billions of users have private conversations protected against passive eavesdropping by the service provider, hackers, and governments without taking any action or even being aware of that protection.

With Signal, each user has a public and private key that the messaging app generates upon installation. Signal implementations rely on a server to relay messages and distribute public keys. When Alice and Bob want to communicate securely, they obtain each other's public key (sometimes referred to as their identity key) and jointly compute a shared key using their identity keys. As Alice and Bob exchange messages, they continue to calculate new shared keys to encrypt each message with a different encryption key. This approach provides forward secrecy, a significant privacy protection property in many state-of-the-art encryption systems.

Even if the encryption key for a message is compromised, the attacker gains access to only a single message and cannot read any previous or future messages using the compromised key.

All deployments of the Signal Protocol rely on a centralized key server trust model. The messaging provider maintains a key server that stores and hands out public keys for all users. Reliance on a trusted key server means that even though Signal protects against passive eavesdropping; users are vulnerable to an active man in-the-middle (MITM) attack.

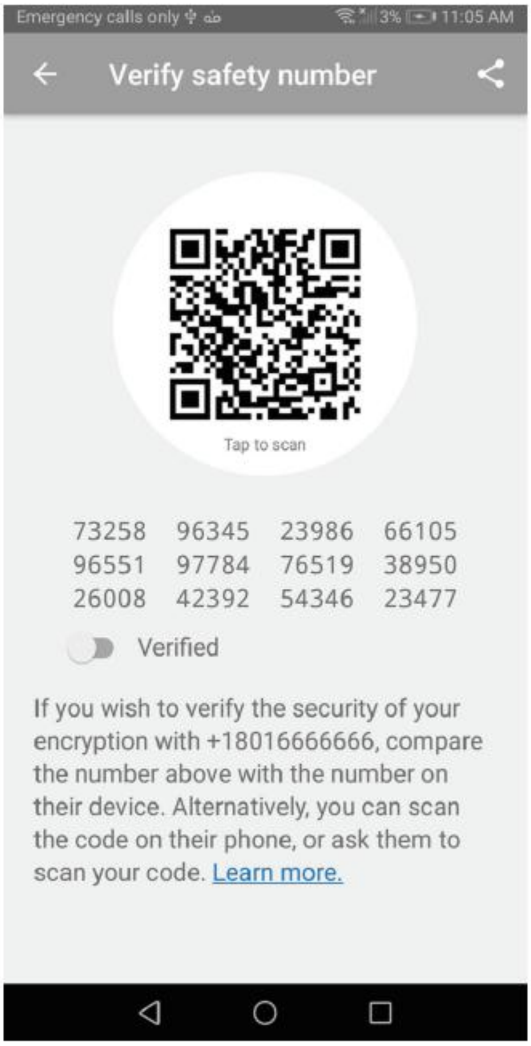
An active MITM attack works as follows. Suppose Alice and Bob want to have a private conversation. A compromised key server can hand out fake keys for Alice and Bob. As Alice and Bob send messages to each other, the compromised server can decrypt and possibly modify each message as it flows through the provider. Alice and Bob are not even aware that their messages are not private.

To defend against an active MITM attack, users can complete an authentication ceremony with each contact to verify out-of-band that their device has the correct public key of their contact and not a fake key from an active MITM attacker. Key verification requires that a pair of users each navigate to an interface in their messaging client and confirm that both users have the same fingerprint (sometimes called a safety number) on their phone as their partner. There are two ways to accomplish key verification. First, if the users are physically co-located, the app provides each with a QR code that they each scan from their partner's phone to confirm that they have each other's correct public key. The QR code confirmation requires that the partners meet and conduct the ceremony in person. If they areremote, they can confirm that they each have the same. One partner can read the safety number to the other partner to confirm. If the numbers match, the conversation is private. If the numbers don't match, an active MITM attack is likely in progress.

The usable security research community has studied the effectiveness of the current authentication ceremony and proposed improvements based on usability study results. There have been studies that compare various methods for comparing fingerprints, along with studies that analyse the full authentication ceremony. More recently, a redesign of the authentication ceremony interface using opinionated design resulted in fewer mistakes and reduced the averagetime to find and complete the ceremony from 11 to 2 min.

XNext, an approach to automate the ceremony by confirming key ownership using social media accounts removed the requirement that both participants be physically present or communicate online while confirming each other’s keys. However, the results show that users do not trust social network providers as the third party to distribute their keys automatically.

XNext, an approach to automate the ceremony by confirming key ownership using social media accounts removed the requirement that both participants be physically present or communicate online while confirming each other’s keys. However, the results show that users do not trust social network providers as the third party to distribute their keys automatically.



73258 96345 23986 66105
96551 97784 76519 38950
26008 42392 54346 23477

If you wish to verify the security of your encryption with +18016666666, compare the number above with the number on their device. Alternatively, you can scan the code on their phone, or ask them to scan your code. Learn more.

7.3 Issues

Lack of user understanding—Users do not understand the need for the authentication ceremony to detect man-in-the-middle attacks.

Authentication ceremony is not usable—Lab studies show that the authentication ceremony is time-consuming, error-prone, and hard to use.

No interoperability—The current IM systems are walled gardens or silos. There is no interoperability between different providers. A WhatsApp user cannot communicate securely with a Facebook Messenger user.

Server must be trusted—The secure messaging provider is trusted to deliver public keys and provide the client software. Even if a user has the assurance that a contact's correct key is in use, there is still the risk that compromised software can leak keys or sensitive information. The government could still coerce a company to update the software on a target's phone with a backdoor.

7.4 Recommendations

Use secure messengers for private communication—For secure communication, the best option available today is for individuals to use an instant messenger client that supports the Signal Protocol for private conversations.

Vulnerable users should complete the authentication ceremony—If you are a high-risk target or are communicating highly sensitive data, complete the authentication ceremony with each contact to ensure there is no MITM attack.

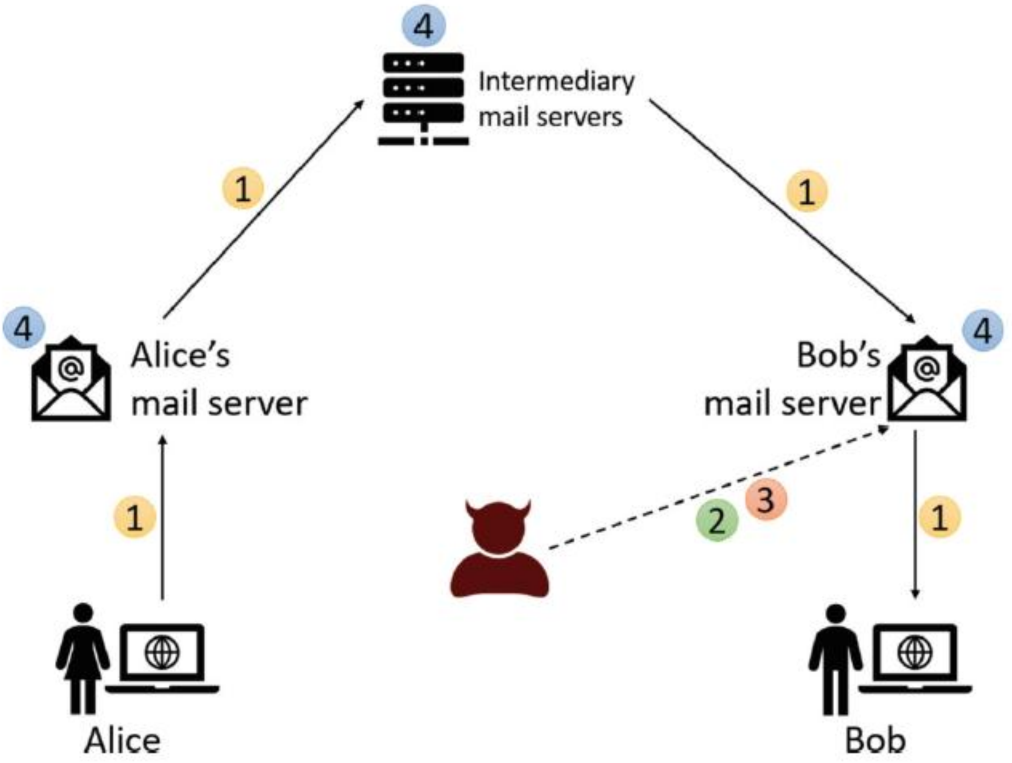
Automate key verification—Design methods to automatically detect or prevent active MITM attacks that relieve users from the burden of the authentication ceremony. Provide application-independent key management—Provide centralized support for key management in the browser or operating system to enable interoperability between applications that support the Signal Protocol. Better support for message deletion—Study user behavior and attitudes in response to new features that allow them to forget or delete messages.

Safeguard encryption keys—Design approaches utilizing secure enclaves to protect encryption keys and encryption software from compromise.

7.5 Secure Email

Email was not originally designed to be secure. Figure illustrates the vulnerabilities in plaintext email, including (1) unsecured links, (2) message forgeries, (3) malicious content, and (4) untrusted servers. Without the use of encryption, sensitive email messages are vulnerable to eavesdroppers while in transit. In addition, sensitive messages stored in the server are also vulnerable to unauthorized access.

Email messages are often stored indefinitely, and the long-term storage adds to the privacy risks even if the data is compromised well into the future. Technologies exist to address some of these vulnerabilities. Transport Layer ecurity (TLS) encrypts email messages during transmission between communication links. Sender Policy Framework (SPF) lets the domain owner specify the legitimate servers that send email messages for that domain. DomainKeys Identified Mail (DKIM) includes a signature on each email message from a domain to guard against message forgery. Recent studies show that these techniques are not universally deployed, leaving a significant gap in the secure email infrastructure. Even if we close this gap, servers still have access to plaintext email messages, and the threat of disclosure to hackers or government surveillance remains.



End-to-end encryption addresses the issue of server access to plaintext email. The most well-known secure email systems are S/MIME and PGP. S/MIME supports a hierarchical, top-down trustmodel and is used mainly in corporations. PGP supports a grass-roots, bottom-up trust model that is suitable for individuals. Deployment of these technologies continues to languish after decades. The reasons are complex and nuanced, and center around a diverse set of stakeholders with competing interests that no one-size-fits-all solution can satisfy.

Secure email is one of the challenges that launched the field of usable security with the seminal paper Why Johnny Can't Encrypt. The paper included a lab usability study of PGP that failed miserably and provided a wake-up call to the security community of the importance of user-centered design. Nearly 20 years later, a lab usability study of a modern PGP web client (Mailvelope) had similarly disappointing results when 9 of 10 participant pairs were unable to exchange a secure email message after 1 h of trying to use the system.

Despite the lack of a usable production PGP tool, recent research has produced several highly usable secure email interfaces. Figure illustrates the interface for Private Webmail 2.0, a system that grew out of a series of studies over many years. The research shows that the following are essential properties for a usable, secure email interface.

Tight Integration. Users want secure email systems that enhance their existing email clients and fit within their existing workflows. This integration is both visual and functional—that is, it looks like a part of the client application and has similar functionality, While visual integration is important, users should be able to clearly distinguish between emails protected with end-to-end encryption and emails that are not.

While most users prefer integrated solutions, a small but consistent portion prefer standalone clients, believing that handling secure email in a separate client makes it more obvious to the user when encryption is in use.

Inline, context-sensitive tutorials. Tutorials are essential in helping users understand how to use secure email properly. For users to pay attention and use these tutorials, the tutorial must be shown inline with the secure email system. Additionally, the system should provide context-sensitive tutorials, walking first-time users through the process of sending and receiving secure email.

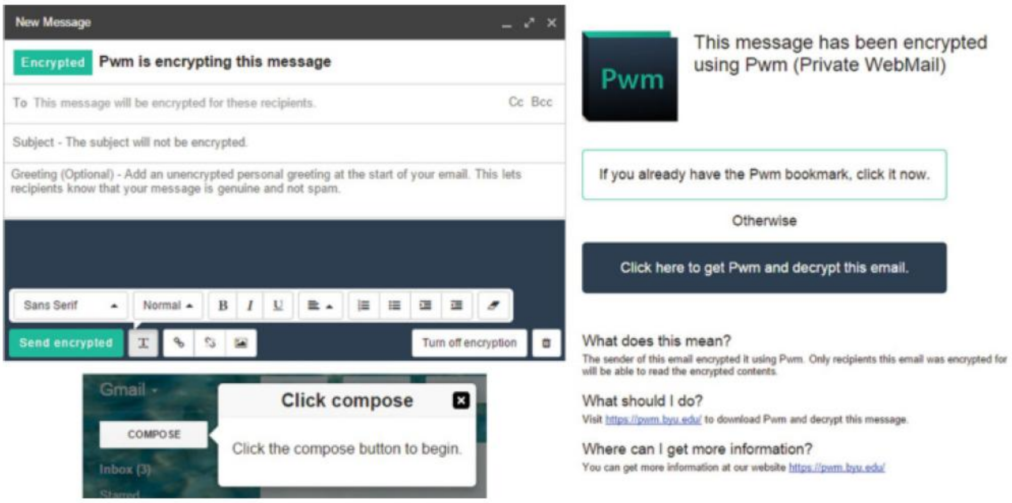
Streamlined onboarding. Encrypted email should be designed to help recipients understand what they have received and what actions they need to take next. If the secure email system requires recipients first to generate a key pair, the system should automatically send an email explaining what the recipient needs to do. Additionally, the system should save a draft of the sender’s message to send automatically after the recipient generates and makes their public key available.

Understandable and trustworthy design. Interfaces need to help users understand how secure email is protecting them—for example, telling them whether the subject line is encrypted (it usually is not). Increased understanding allows users to make informed decisions and avoid mistakes. Additionally, system operation needs to conform to user expectations; otherwise, users reject the system. For example, studies show that if encryption happens too quickly, users assume that their messages were not encrypted and did not trust the tool.

Easy-to-use key management. Users struggle with managing their keys. Automation of key generation, uploading, and discovery significantly improve the user experience.

Studies show that systems applying (most of) these principles are perceived as highly usable, result in a low mistake rate, and help novice users begin sending encrypted email without expert assistance.

Secure email is a two-body problem, pioneered a novel two-person methodology where pairs of participants are brought into a user study to test a system. They found that participants were more relaxed during the study and



Pwm is encrypting this message

To This message will be encrypted for these recipients.

Subject - The subject will not be encrypted.

Greeting (Optional) - Add an unencrypted personal greeting at the start of your email. This lets recipients know that your message is genuine and not spam.

Click compose

Click the compose button to begin.

This message has been encrypted using Pwm (Private WebMail)

If you already have the Pwm bookmark, click it now.

What does this mean?

The sender of this email encrypted it using Pwm. Only recipients this email was encrypted for will be able to read the encrypted contents.

What should I do?

Visit https://pwm.byu.edu/ to download Pwm and decrypt this message.

Where can I get more information?

You can get more information at our website https://pwm.byu.edu/

Top left—placeholder text that acts as an inline tutorial instructing users about how secure email works. Bottom left—an inline, context-sensitive tutorial helping users send an encrypted email for the first time.

Right—the body of the encrypted email providing plaintext instructions to streamline onboarding. Interface for private webmail (Pwm) 2.0, a modern usable secure email system did not automatically assume that they were responsible for system mistakes.

The storage of plaintext email at the server presents an attack surface in case of future account compromise. Research is beginning to explore email deletion capabilities that reduce the risk of future disclosure of sensitive messages that do not require long-term storage. Another approach is to encrypt the plaintext email on the server with a locally stored encryption key and delete the plaintext copy. The advantage of this approach is that a user can do this unilaterally without the cooperation of their communication partner. However, it does not safeguard the copy of the message in the original sender's outbox.

Multiple stakeholders with competing priorities for secure email make it difficult for a one-size-fits-all solution. There needs to be more willingness by the various stakeholders to allow for alternatives that support the needs of only some of the stakeholders. There has been significant effort by the usable security research community to study the issues surrounding secure email, and usable system designs have been demonstrated in a laboratory setting.

Issues

PGP is dead—PGP is a failed experiment. Even the proponents of secure email have been abandoning PGP recently. Modern PGP clients exhibit poor usability in laboratory user studies.

Secure email solutions are not interoperable—The various approaches to secure email are not interoperable (PGP, S/MIME, proprietary web-based systems).

It is difficult to introduce a secure email solution that maintains ubiquity—Email has a history emphasizing ubiquity and interoperability. Anyone can send an email to any other user if they have an email address for them. It is challenging to introduce secure email into this environment and maintain the same service guarantees.

7.6 Recommendations

Individuals should use secure messaging instead—Given the current state of secure email, use a secure messaging client that supports the Signal Protocol for private conversations with friends and family.

Businesses should use S/MIME or secure webmail—For sensitive business communications that must occur over email, enterprises can use S/MIME, and small businesses and individuals can use web-based secure email services such as ProtonMail and Tutanota.

All email providers should support TLS—It is exasperating that all email is not protected from passive eavesdropping today. All email systems should support TLS for exchanging email between email systems.

Delete old sensitive email when possible—Unless legally required to retain a copy, delete outdated sensitive email messages that could be problematic if made public following an account compromise.

Longitudinal studies are needed—Previous secure email usability studies are all short-term lab studies. Longitudinal studies could confirm whether the above design principles are sufficient for email or whether more improvements are needed to support long-term usage.

Providers should only have access to encrypted messages—Develop techniques to process encrypted data so the email provider can scan for malware and spam without having access to the plaintext.

Support easy deletion of old messages—Analyze the usability of secure email deletion approaches.

7.7 HTTPS

The privacy of sensitive information is protected when it is encrypted during transmission over an insecure network. HTTPS is the protocol for encrypting data transmitted between browsers and web servers. It relies on a lower-level protocol known as Transport Layer Security (TLS), formerly known as the Secure Socket Layer (SSL). At a high level, HTTPS/TLS/SSL are synonymous—it is the most common protocol for encrypted communication on the Internet. As part of the HTTPS setup, a website authenticates to the browser using a certificate digitally signed by a trusted third party.

In 2010, the Firesheep browser extension demonstrated the risks of session hijacking for sites that used HTTPS only to protect the login page and sent browser cookies in the clear. The tool allowed an attacker sniffing traffic on a wireless network to easily hijack another user's session to gain unauthorized access to their social network or webmail. The publicity and ease of performing this attack contributed to major websites, like Google and Facebook, requiring HTTPS for all session traffic to their website.

More recently, there has been a significant uptick in the use of HTTPS for all web traffic, which provides increased protection against unauthorized access to browser activity. The increase in HTTPS has been mainly fueled by Let's Encrypt, a service that offers free digital certificates that are easy for admins to request and manage.

The most recent version of the protocol (TLS 1.3) supports only ciphers that provide the forward secrecy property described earlier in the secure messagingdiscussion. It also provides increased privacy protection by encrypting the server certificates transmitted to the client. There are three aspects of HTTPS that have socio-technical implications: (1) TTPS warning messages, (2) developer and administrator development and deployment hurdles, and (3) HTTPS inspection.

7.8 HTTPS Warning Messages

Users are sometimes faced with HTTPS warning messages when the browser encounters a website certificate that does not properly validate. The web servercertificate authenticates a website to the browser. HTTPS warnings have been an area of significant usability studies and modification over the past decade. Researchers at Google have been at the forefront of this effort. Google is well-positioned to gather telemetry data from its users and conduct large-scale A/B tests comparing alternate designs. The results of these studies have shown a decrease in the click-through rate of HTTPS warning messages. It isn't clear that the reduction is due to increased user understanding as much as it is that the browsers make it more difficult to click through the warning message by adding additional steps that may discourage users from continuing.

Browsers display a lock icon whenever HTTPS is in use. Users interpret the lock icon as an indicator that the website is secure. Several studies show that users interpret the lock icon to mean that the website is secure. The lock icon is unrelated to the website’s security, and this misunderstanding is precisely the wrong interpretation when a phishing website impersonates a well-known company and employs HTTPS.

7.9 HTTPS Development and Deployment

Software developers that build HTTPS applications can make mistakes, such as introducing certificate validation errors that compromise user privacy. Two recent research projects presented user-level and system-level approaches for automatically intercepting and verifying a website certificate, which overrides an application with broken HTTPS authentication. An approach that goes beyond intercepting brokenHTTPS applications is to design amore straightforward, abstract interface to HTTPS applications that make it easier for developers to build reliable applications that encrypt network traffic. a simple extension to the existing POSIX secure socket API.

Administrators of websites can misconfigure HTTPS and create privacy risks for users. A qualitative study examined mental models of users and administrators, and administrators did not understand protocol components and technical terms associated with HTTPS.

7.10 HTTPS Interception

HTTPS interception (also known as a TLS Proxy) often occurs within a corporation, library, or school so that the organization can monitor the security of their network and make sure clients are not unknowingly downloading malware or releasing sensitive business secrets from a compromised machine. Several studies measure how often HTTPS inspection occurs by using detection techniques from the server side. A study of client-side HTTPS interception software shows that these systems can introduce privacy risks to users due to programmer error.

The same mechanisms utilized for inspection can also be the source of an active man-in-the-middle attack. Since the two options appear similar, it makes the task of informing the user all the more difficult.

7.11 Issues

Companies perform HTTPS Interception to protect their network and systems. Intermediate servers run by a company or organization can access a user’s HTTPS web traffic, known as HTTPS inspection. Some users consider this a privacy breach, but they understand why a company must protect its network.

Users overwhelmingly desire notification when an HTTPS proxy is operating.

Many HTTPS applications are broken. Developers make mistakes when building HTTPS applications due to the complexity of HTTPS libraries.

7.12 Recommendations

Use HTTPS on all websites. All owners of websites should be using HTTPS for all connections to their site. Certificates are inexpensive and easy to acquire using Let’s Encrypt.

Website designers should not mix HTTP and HTTPS traffic on a single web page since this has been a source of compromise in the past.

7.13 Check Your Progress

1. Describe secure messaging and explain how end-to-end encryption and the Signal Protocol protect user privacy.
2. What is a Man-in-the-Middle (MITM) attack in secure messaging? Explain the authentication ceremony used to prevent it and its limitations.
3. Discuss the major issues and recommendations related to secure email, highlighting why secure email adoption remains challenging.
4. Explain HTTPS and its role in protecting data during transmission. Discuss the usability issues related to HTTPS warning messages.
5. What is Two-Factor Authentication (2FA)? Explain its importance, common usability issues, and recommendations for improving user adoption.

UNIT- 8
Privacy and Security in Social Media

8.1 OBJECTIVES

After completing this unit, students will be able to:

- Understand the concept of privacy and security in social media and their importance in daily digital life.
- Explain the meaning of privacy and security in social media platforms with suitable examples.
- Identify various privacy issues and security threats associated with social media usage.
- Analyse the importance of protecting personal information from misuse, cybercrime, and identity theft.
- Describe different ways and best practices to protect privacy and security on social media platforms.
- Develop safe and responsible online behaviour for effective and secure use of social media.

8.2 INTRODUCTION

Social media has become an essential part of modern life, allowing people to communicate, share information, and build communities across the world. Platforms such as social networking sites, messaging apps, and content-sharing services make it easy to connect with others instantly. However, along with these benefits come serious concerns about privacy and security. Users often share large amounts of personal information online, which can be misused if not properly protected. Understanding privacy and security in social media is important to ensure safe and responsible use of these platforms.

8.3 MEANING OF PRIVACY IN SOCIAL MEDIA

Privacy in social media refers to the protection of users' personal information, such as names, photos, locations, contact details, and personal opinions. It also includes controlling who can see, share, or use this information. Many users are unaware that their data may be collected, stored, and sometimes shared with third parties without explicit consent.

Why Privacy Matters

Social media platforms like Facebook, Instagram, Twitter (now X), and TikTok thrive on user-generated content, but this comes at the cost of privacy. Every like, comment, share, or post creates a digital footprint that platforms analyze using algorithms. This data fuels targeted advertising, but it can also lead to misuse, such as identity theft, stalking, or discrimination. For instance, in 2018, the Cambridge Analytica scandal revealed how Facebook data from 87 million users was harvested to influence elections, highlighting how "free" services monetize personal info.

Common Privacy Risks

Data Collection: Platforms track not just what you post, but also your browsing habits, device info, and even microphone/camera access via apps.

Third-Party Sharing: Apps and advertisers access your data through APIs; a simple quiz app might pull your friend list and location.

Cyber Threats: Hackers exploit weak privacy settings for phishing, doxxing (publicly exposing private info), or ransomware.

Government Surveillance: In countries like India, laws like the IT Rules 2021 require platforms to trace user data, balancing security with privacy erosion.

How Platforms Handle Privacy

Most sites offer privacy settings—like "friends only" posts or two-factor authentication—but defaults are often public to boost engagement. Features like Stories (temporary posts) or end-to-end encryption in WhatsApp help, yet metadata (e.g., who you message) remains visible. Regulations like GDPR in Europe or India's DPDP Act 2023 aim to enforce consent and data minimization, giving users rights to delete or port their data.

Tips for Protecting Your Privacy

Adjust settings: Make profiles private, limit app permissions, and review tagged photos.

Use tools: Enable VPNs, incognito mode, or privacy-focused apps like Signal.

Be mindful: Avoid oversharing; think "Would I say this in public?"

Stay informed: Regularly update apps and read privacy policies (short versions exist on most sites).

Ultimately, true privacy requires user vigilance alongside better platform accountability. In an interconnected world, safeguarding your digital self prevents real-world harm.

8.4 MEANING OF SECURITY IN SOCIAL MEDIA

Security in social media involves protecting accounts and data from unauthorized access, cyberattacks, hacking, identity theft, and online fraud. Strong security measures help prevent criminals from misusing user accounts or stealing sensitive information, ensuring users can interact safely without fear of exploitation.

Why Security Matters

Social media is a prime target for cybercriminals due to its vast user base—over 5 billion globally, including 500+ million in India. Weak security doesn't just risk personal data; it enables scams like fake giveaways or phishing that spread malware. High-profile breaches, such as the 2021 Facebook hack affecting 533 million users (including leaked Indian phone numbers), show how one vulnerability cascades into mass harm.

Common Security Threats

Phishing Attacks: Fake login pages trick users into entering credentials.

Account Takeovers: Password stuffing (reusing stolen passwords) or SIM-swapping to hijack 2FA.

Malware and Ransomware: Malicious links in DMs encrypt devices for ransom.

Social Engineering: Scammers pose as friends to extract info or money.

DDoS Attacks: Overloading platforms to disrupt services, as seen in assaults on Twitter.

Key Security Mechanisms

Platforms deploy layered defenses:

Authentication: Multi-factor authentication (MFA), biometrics, and passwordless logins.

Encryption: HTTPS for data in transit; end-to-end for messages (e.g., WhatsApp).

AI Monitoring: Algorithms detect suspicious logins from new devices or locations.

Compliance: Adhering to standards like ISO 27001 or India's CERT-In guidelines for breach reporting within 6 hours.

Best Practices for Users

- Use strong, unique passwords managed by tools like password managers (e.g., Bitwarden).
- Enable MFA everywhere and avoid SMS-based (opt for app authenticators).
- Verify links before clicking; report suspicious activity promptly.
- Keep apps updated and use antivirus software.
- Limit third-party app access via settings.

In essence, social media security is a shared responsibility—platforms provide tools, but users must adopt them proactively to counter evolving threats.

8.5 PRIVACY ISSUE IN SOCIAL MEDIA

Oversharing of personal information: Users post details like home addresses, phone numbers, or routines (e.g., "Live from my favorite café!"), inviting stalkers or burglars.

Data collection without user awareness: Platforms harvest metadata like IP addresses, contacts, and browsing history via cookies and trackers, often buried in lengthy terms of service.

Tracking of user activities: "Like" buttons and pixels on external sites follow you across the web, building detailed profiles sold to advertisers.

Misuse of personal photos and videos: Images can be deepfaked, revenge-porned, or used in catfishing scams without consent.

Lack of control over shared content: Once posted, content can be screenshotted, shared indefinitely, or algorithmically amplified beyond your network.

These issues can lead to loss of privacy, reputation damage, emotional stress, identity theft, or even physical harm—like the 2014 case of a Delhi teen stalked via Instagram geotags.

8.6 SECURITY THREATS

Social media users face several security threats, such as:

Hacking and account takeover: Cybercriminals use credential stuffing or brute-force attacks to seize control, then post spam or demand ransom (e.g., 2022 Twitter hack of high-profile accounts).

Phishing attacks and fake links: Deceptive messages mimic friends or brands, tricking users into fake login pages (e.g., "Your account is suspended—click here").

Malware and spyware: Infected links or apps install keyloggers to steal data; mobile malware rose 30% in India in 2025 per CERT-In.

Identity theft: Stolen profiles enable impersonation for scams or reputational harm.

Online scams and fraud: Fake giveaways, romance scams, or job offers extract money—India lost ₹1,200 crore to such frauds in 2024.

Weak passwords and careless clicking often increase these risks, amplifying vulnerabilities in platforms handling billions of daily interactions.

Additional Security Threats

SIM Swapping: Attackers hijack phone numbers to bypass 2FA, accessing linked accounts.

DDoS Attacks: Flood platforms to crash services, enabling theft during chaos.

Social Engineering: Manipulating users via DMs to reveal info (e.g., "Send OTP for verification").

Ransomware: Locks devices after clicking malicious ads, demanding crypto payment.

Man-in-the-Middle (MitM) Attacks: Intercept unencrypted Wi-Fi data on public networks.

8.5 IMPORTANCE OF PRIVACY AND SECURITY

Protecting privacy and security on social media is important because it:

Safeguards personal and financial information: Prevents leaks of addresses, bank details, or health data that could lead to fraud.

Prevents cybercrimes and online harassment: Stops hacking, doxxing, or bullying that affects mental health—1 in 5 Indian teens report cyberbullying per NCRB 2025.

Maintains user trust and safety: Builds confidence in platforms, encouraging positive engagement without fear.

Protects individuals from identity theft and misuse of data: Blocks scammers from impersonating you or selling profiles on dark web markets.

Additional Key Reasons

Preserves Reputation and Career: Old posts can resurface, costing jobs (e.g., 2024 cases of influencers blacklisted over leaked data).

Supports Mental Well-Being: Reduces anxiety from constant surveillance or unwanted exposure.

Enables Regulatory Compliance: Aligns with laws like India's DPDP Act 2023, avoiding fines up to ₹250 crore for platforms.

Fosters Innovation: Secure environments promote features like secure payments (e.g., Instagram Shopping) without breach fears.

National Security: Curbs misinformation or foreign interference, as seen in 2024 election hacks.

8.6 WAYS TO PROTECT PRIVACY AND SECURITY

Using strong and unique passwords: Combine letters, numbers, symbols (e.g., "Sm@rtAss@m2026!"); avoid "123456" or birthdays.

Enabling two-factor authentication (2FA): Adds a code from an app like Google Authenticator—blocks 99% of automated hacks.

Adjusting privacy settings: Switch to "friends only," disable search engine indexing, and review tagged content.

Avoiding suspicious links and messages: Hover to check URLs; use scanners like VirusTotal.

Limiting the sharing of personal information: Skip posting addresses, schools, or routines; use vague terms like "out and about."

Logging out from public devices: Clear cookies and use incognito mode on cyber cafés or shared PCs.

Privacy-Focused Actions

Regular Audits: Monthly check who sees your posts; delete inactive accounts.

Ephemeral Sharing: Use disappearing messages (e.g., WhatsApp) or Stories.

Data Minimization: Opt out of ad tracking via settings (e.g., "Off-Facebook Activity").

Security-Focused Actions

Software Updates: Enable auto-updates to patch vulnerabilities—critical after 2025 Log4j exploits.

Antivirus and VPNs: Install apps like Norton or ExpressVPN, especially on public Wi-Fi.

Device Security: Use biometric locks and encrypt phones.

Awareness and Reporting

Verify Before Engaging: Confirm friend requests; ignore unsolicited prizes.

Report Incidents: Use platform tools or India's National Cyber Crime portal (cybercrime.gov.in).

Educate Yourself: Follow CERT-In alerts and BAOU cybersecurity modules.

Tools and Resources Table

8.7 CHECK YOU PROGRESS

- Explain the meaning of privacy and security in social media with examples. Discuss common privacy issues like oversharing and data collection, and how they lead to real-world harm such as identity theft or stalking.

- Describe five major security threats in social media (e.g., phishing, malware, account takeover). Provide examples from India (like CERT-In reported incidents) and their consequences for users.

- Why is protecting privacy and security crucial on social media? Elaborate on benefits like preventing cybercrimes, maintaining trust, and compliance with laws such as India's DPDP Act 2023.

- Outline at least eight ways to protect privacy and security (e.g., strong passwords, 2FA, privacy settings). Explain how each works and recommend tools like Bitwarden or VPNs with step-by-step implementation.

- Differentiate between privacy risks (e.g., tracking, photo misuse) and security threats (e.g., hacking, scams). Suggest integrated measures for BAOU students using social media for education.

Fill in the Blanks

__________ authentication uses a second factor like an app code to secure accounts.
Answer: Two-factor (or 2FA)

Platforms collect user data via __________ and cookies without always informing users.
Answer: Tracking

__________ swapping hijacks phone numbers to bypass account security.
Answer: SIM

Always __________ out from public devices to prevent unauthorized access.
Answer: Log

India's __________ Act 2023 mandates consent for data processing in social media.
Answer: DPDP

BLOCK -2

UNIT – 5

Privacy in Social Media

Unit Structure

5.1 OBJECTIVE

After this unit, students will be able to:

- Define privacy and explain its 7 dimensions with Indian examples.
- Distinguish digital footprint types and manage online identity risks.
- Analyze data collection methods, profiling uses, and 6 ethical concerns.
- Identify 7 social media privacy risks and apply 15+ preventive measures.
- Apply legal frameworks (IT Act, DPDP) and security practices for safe usage.

5.2 INTRODUCTION

In the digital age, people use the internet for communication, education, banking, shopping, entertainment, and social networking. While these technologies provide convenience and connectivity, they also raise serious concerns about **privacy**. Personal information such as name, location, photos, preferences, and online behaviour is constantly collected, stored, and shared. Understanding digital privacy is essential to protect individuals from misuse of personal data, identity theft, surveillance, and cybercrime.

5.2 MEANING AND DIMENSIONS OF PRIVACY

Meaning of Privacy

Privacy refers to an individual's right to control their personal information and decide how, when, and to what extent it is shared with others. It encompasses not just data but also personal autonomy, protecting against unwanted intrusion into one's life, body, or decisions. This right is foundational in legal frameworks like India's Article 21 (right to life and personal liberty) and global standards such as the GDPR in Europe.

Dimensions of Privacy

- **Information Privacy**: Protection of personal data such as name, phone number, Aadhaar number, financial details, and medical records. This dimension focuses on preventing unauthorized collection, storage, or sharing of identifiable information, often safeguarded by laws like India's Digital Personal Data Protection Act (DPDP), 2023.

- **Communication Privacy**: Privacy of emails, messages, phone calls, and online chats. It ensures confidentiality in interpersonal exchanges, shielding against eavesdropping, data interception, or compelled disclosure, as protected under telecom regulations and encryption standards.
- **Physical Privacy:** Protection from physical surveillance, such as CCTV misuse or unauthorized tracking. This includes safeguards against unwarranted searches, home intrusions, or biometric monitoring without consent, balancing public safety with individual rights.
- **Decisional Privacy:** Freedom to make personal choices without external interference (e.g., beliefs, lifestyle choices). This dimension empowers individuals to form intimate relationships, religious convictions, reproductive decisions, and family matters privately, free from state or societal coercion.
- **Additional aspects include:**

Bodily Privacy: Autonomy over one's body, such as consent for medical procedures, vaccinations, or gender-affirming care. For instance, forcing medical treatments without informed consent violates this, as seen in debates over mandatory health policies.

Relational Privacy: The right to choose associations, like marriage, friendships, or sexual orientation, without judgment or penalty. India's Supreme Court recognition of privacy.

Associational Privacy: Freedom to join groups, unions, or political parties privately, protecting against surveillance of memberships that could lead to discrimination.

Locational Privacy: Control over tracking one's movements via GPS or apps, preventing inferences about habits or routines.

These dimensions often overlap - for example, sharing location data (information privacy) can reveal lifestyle choices (decisional privacy). In India, evolving jurisprudence like the Puttaswamy judgment (2017) affirms privacy as intrinsic to dignity.

5.3 DIGITAL FOOTPRINT AND ONLINE IDENTITY

Digital Footprint

A digital footprint is the trail of data created by users while using the internet. It persists across platforms and can influence opportunities like jobs or loans, often outlasting the user's control. In India, with over 900 million internet users (as of 2025), managing this footprint is crucial under laws like the DPDP Act.

Types of Digital Footprint

Active Digital Footprint: Data shared intentionally (posts, comments, form submissions). Examples include uploading photos on Instagram or filling out e-commerce profiles.

Passive Digital Footprint: Data collected without direct user awareness (cookies, tracking, and browsing history). This includes IP logs, device fingerprints, and geolocation from apps, often used for targeted ads.

Online Identity

Online identity is how a person is represented on the internet, including social media profiles, email accounts, usernames, and avatars. It shapes perceptions by others and can be fragmented across platforms or deliberately curated (e.g., via pseudonyms). Unlike real-world identity, it's malleable but vulnerable to hacking or misrepresentation.

Key components and aspects include:

- **Social Media Profiles:** Curated personas on platforms like Facebook, Instagram, or X (formerly Twitter), revealing interests, networks, and timelines.
- **Email Accounts and Digital Signatures:** Gateways to services, often linked to verified identities via two-factor authentication.
- **Usernames and Avatars:** Digital handles and visuals that signal personality, anonymity, or branding (e.g., gamer tags on Discord).
- **Online Behaviour and Reputation:** Patterns like posting frequency, engagement style, or review history that build a "reputation score." Tools like Google searches or Klout scores quantify this.
- **Biometric and Verified Identities:** Linked accounts via Aadhaar, UPI handles, or facial recognition on apps like WhatsApp.
- **Shadow Profiles:** Invisible data aggregates (e.g., Facebook's inferred profiles from friends' data) that exist without user knowledge.

Risks and Management

Online identities can lead to doxxing, identity theft, or biased algorithms (e.g., denied loans due to old posts). To manage: Use privacy settings, VPNs, delete old accounts via tools like JustDeleteMe, and monitor with services like Have I Been Pwned? Example: In 2023, a viral LinkedIn post cost a job seeker an offer due to mismatched online behaviour. These concepts intersect with privacy - your digital footprint forms the basis of your online identity, amplifying risks in India's growing digital economy.

5.4 DATA COLLECTION AND USER PROFILLING

Data Collection

Organizations collect user data through various digital touchpoints to fuel business models and services. This data forms the backbone of the modern internet economy.

Methods include:

- Cookies and trackers (e.g., third-party pixels from Google Analytics).
- Online forms (e.g., sign-ups capturing emails and preferences).
- Social media interactions (e.g., likes, shares on Meta platforms).
- Mobile apps and GPS (e.g., location pings from Uber or Swiggy).

User Profiling

User profiling is the process of analyzing collected data to understand user behavior, interests, preferences, and habits. It uses AI and machine learning to create detailed "user personas," often scoring users on traits like purchase likelihood or political leanings.

Uses of User Profiling

Targeted advertising (e.g., showing shoe ads after browsing sneakers).

Personalized content (e.g., Netflix tailoring watchlists).

Recommendation systems (e.g., Amazon's "customers also bought").

Market research (e.g., predicting trends from aggregated habits).

Concerns

While beneficial, user profiling raises serious ethical and legal issues, often prioritizing profits over rights.

Expanded concerns include:

Loss of Privacy: Constant surveillance erodes anonymity; passive data like browsing history reveals sensitive details without consent. Example: Cambridge Analytica scandal (2018) exposed how Facebook data profiled 87 million users for elections.

Manipulation of User Behavior: Algorithms nudge choices via filter bubbles or addictive feeds, exploiting psychological biases (e.g., TikTok's "For You" page keeping users scrolling).

Discrimination: Biased profiles perpetuate inequality; facial recognition misidentifies darker skin tones, or credit scoring disadvantages low-income groups. In India, this affects Aadhaar-linked services.

Data Misuse and Breaches: Hacked profiles lead to identity theft or blackmail; sold data fuels spam or fraud. 2024's massive AT&T breach exposed 73 million profiles.

Lack of Transparency and Consent: "Dark patterns" trick users into sharing (e.g., pre-checked boxes); profiling happens invisibly via cross-site tracking.

Surveillance Capitalism: Companies like Google monetize predictions of behavior, commodifying personal lives.

Legal and Mitigation Measures
India's DPDP Act (2023) mandates consent, data minimization, and rights like erasure. Globally, GDPR fines (e.g., €1.2B on Meta in 2023) enforce accountability. Users can opt for privacy-focused browsers (e.g., DuckDuckGo), ad blockers, or tools like Privacy Badger. Example: Apple's App Tracking Transparency (2021) lets users block profiling, slashing ad revenues.
These practices highlight the tension between innovation and individual control in a data-driven world.
Here's an expanded version of your outline on "Privacy Risks in Social Media." I've fleshed out each risk with explanations, examples, and impacts, then added a detailed "Preventive Measures" section with practical steps, stats, and an illustrative example for completeness.

5.6 Privacy Risks in Social Media

Social media platforms pose several privacy risks due to their vast data collection, public sharing defaults, and interconnected ecosystems. With India's 500+ million users (2025 stats), these risks amplify in diverse contexts like family networks or political discourse.

Key Privacy Risks

Oversharing Personal Information: Users post details like addresses, routines, or family photos impulsively, enabling strangers to piece together profiles.

Impact: Leads to burglary (e.g., "empty house" posts during vacations).

Identity Theft: Stolen credentials or profile data allow impersonation for scams or fraud. Example: Phishing via fake friend requests.

Cyberstalking and Harassment: Trackers exploit posts to monitor locations or harass (e.g., doxxing on X/Twitter). India's 2024 NCRB data shows rising cyberstalking cases.

Data Breaches: Hacks expose millions of records; 2023 Meta breach leaked 6TB of user data.

Facial Recognition Misuse: Auto-tagging scans faces without consent, feeding surveillance databases (e.g., Clearview AI controversies).

Third-Party App Access: "Log in with Facebook" grants apps broad data permissions, often forgotten and revocable only manually.

Location Tracking: Check-ins or geotags reveal real-time movements, risking safety (e.g., stalkers using Instagram Stories).

Preventive Measures Protect yourself with proactive habits and tools:

Privacy Settings: Set profiles to private, limit post visibility (e.g., "Friends only" on Facebook), and disable location services. Review monthly.

Minimize Sharing: Avoid posting sensitive info; use Stories that auto-delete instead of permanent feeds. Think "STRANGER test"—would you share with a stranger?

Strong Authentication: Enable 2FA, unique passwords via managers like LastPass, and biometric locks.

App Permissions: Revoke third-party access regularly (e.g., Facebook's "Apps and Websites" section); deny unnecessary permissions.

Tools and Features: Use VPNs (e.g., ExpressVPN), ad blockers, and platform tools like Instagram's "Close Friends." Opt out of facial recognition where possible.

Awareness and Reporting: Educate on phishing; report violations promptly (e.g., Twitter's harassment tools). In India, use cybercrime.gov.in for complaints.

Digital Hygiene: Regularly delete old posts/accounts; use ephemeral apps like Signal for sensitive chats.

5.7 Preventive Measures

Protect your privacy through layered habits, tools, and awareness. These steps minimize risks like data breaches, stalking, and profiling across apps and platforms.

Core Practices

Strong Privacy Settings: Customize platform defaults—set social media to private, limit audience (e.g., Facebook "Friends only"), and disable public searchability. Review quarterly.

Two-Factor Authentication (2FA): Add a second verification layer (e.g., app like Google Authenticator or SMS); enables on Gmail, Instagram. Reduces account hacks by 99% (Google stats).

Avoid Sharing Sensitive Data: Skip posting addresses, Aadhaar, financials, or routines; use vague terms like "out with friends" instead of locations.

Regular Password Updates: Change every 3-6 months; use 12+ character passphrases (e.g., "BlueHorseBatteryStaple") via managers like Bitwarden or 1Password. Avoid reuse.

Advanced Strategies

Awareness of Fake Profiles: Verify via reverse image search (Google Lens), mutual connections, or blue ticks. Report/block suspicious accounts immediately.

Permission Management: Audit app permissions (e.g., revoke camera/mic access); use "Log in with Google" sparingly and review linked apps.

Data Minimization Tools: Employ ad blockers (uBlock Origin), tracker blockers (Privacy Badger), and VPNs (ProtonVPN) to cut passive tracking.

Device and Software Hygiene: Keep OS/apps updated, use antivirus (e.g., Malwarebytes), and enable full-disk encryption (BitLocker on Windows).

Digital Footprint Cleanup: Delete old posts/accounts with tools like JustDeleteMe; request data deletion under DPDP Act or GDPR. Monitor breaches via Have I Been Pwned.

Education and Backup: Stay informed via resources like India's Cyber Swachhta Kendra; back up data securely before resets.

Illustrative Example: A user hit by a 2025 LinkedIn phishing scam enabled 2FA, switched to a password manager, and scanned for fakes—preventing further breaches and recovering their profile safely.

Consistency is key: Treat privacy like hygiene—daily habits yield long-term protection.

5.8 Check Your Progress

1. Define privacy and explain its major dimensions with suitable Indian examples.
2. What is a digital footprint? Explain its types and discuss how it affects online identity.
3. Explain the concept of online identity and discuss the risks associated with managing online identity.
4. Describe the methods of data collection and explain how user profiling is carried out by organizations.

5. Discuss the ethical concerns related to data collection and user profiling with relevant examples.

6. Explain the major privacy risks in social media and describe the preventive measures users can take to protect their privacy.

UNIT : 6

Social Media and Privacy

Unit Structure

6.0 Objective

After completing this unit, students will be able to:

- Understand how social media has changed communication and affected personal privacy.
- Explain the privacy paradox and factors influencing online self-disclosure.
- Analyze social media privacy using the boundary regulation perspective.
- Identify and explain different types of privacy boundaries on social media.
- Understand individual differences in privacy attitudes and their impact on platform design.
- Evaluate privacy challenges, social disenfranchisement, and guidelines for designing privacy-sensitive social media platforms.

6.1 Introduction

The way people communicate with one another in the twenty-first century has evolved rapidly. In the 1990s, if someone wanted to share a “how-to” video tutorial within their social networks, the dissemination optionswould be limited (e.g., email, floppy disk, or possibly a writeable compact disc). Now, social media platforms, such as TikTok, provide professional grade video editing and sharing capabilities that give users the potential to both create and disseminate such content to thousands of viewers within a matter of minutes. As such, social media has steadily become an integral component for how people capture aspects of their physical lives and share them with others. Social media platforms have gradually altered the way many people live, learn, and maintain relationships with others.

6.2 Privacy Paradox

While researchers have investigated these various privacy attitudes, perceptions, and behaviors, the privacy paradox (where behavior does not match with stated privacy concerns) has been especially salient on social media. As a result, much research focuses on understanding the decision-making process behind selfdisclosure. Scholars that view disclosure as a result of weighing the costs and the benefits of disclosing information use the term “privacy calculus” to characterize this process. Other research draws on the theory of bounded rationality to explain how people’s actions are not fully rational. They are often guided by heuristic cues which do not necessarily lead them to make the best privacy decisions. Indeed, a large body of literature has tried to dispel or explain the privacy paradox.

6.3 Reconceptualizing Social Media Privacy as Boundary Regulation

By reconceptualizing privacy in social media as a boundary regulation, we can see that the seeming paradox in privacy is actually a balance between being too open or disclosing too much and being too inaccessible or disclosing too little. The latter can result in social isolation which is privacy regulation gone wrong.

In the context of social media, there are five different types of privacy boundaries that should be considered. People use various methods of coping with privacy violations, many not tied to disclosing less information. Drawing from Altman’s theories of privacy in the offline world, Palen and Dourish describe how, just like in the real world, social media privacy is a boundary regulation process along various dimensions besides just disclosure. Privacy can also involve regulating interactional boundaries with friends or followers online and the level of accessibility one desires to those people. For example, if a Facebook user wants to limit the people that can post on their wall, they can exclude certain people. Research has identified other threats to interpersonal boundary regulation that arise out of the unique nature of social media. First, as mentioned previously, the threat to spatial boundaries occurs because our audiences are obscured so that we no longer have a good sense of whom we may be interacting with. Second, temporal boundaries are blurred because any interaction may now occur asynchronously at some time in the future due to the virtual persistence of data. Third, multiple interpersonal spaces are merging and overlapping in a way that has caused a “steady erosion of clearly situated action”. Since each space may have different and, at times, mutually exclusive behavioral requirements, acting accordingly within those spaces has become more of a challenge to manage context collapses. Along with these problems, a major interpersonal boundary regulation challenge is that social media environments often take control of boundary regulation away from the end users. For instance, Facebook's popular "Timeline" automatically (based on an obscure algorithm) broadcasts an individual's content and interactions to all of his or her friends. Thus, Facebook users struggle to keep up to date on how to manage interactions within these spaces as Facebook, not the end user, controls what is shared with whom.

6.4 Boundary Regulation on Social Media

One conceptualization of privacy that has become popular in the recent literature is viewing privacy on social media as a form of interpersonal boundary regulation. These scholars have characterized privacy as finding the optimal or appropriate level of privacy rather than the act of withholding self-disclosures. That is, it is just as important to avoid over disclosing as it is to avoid under disclosing. Therefore, disclosure is considered a boundary that must be regulated so that it is not too much or too little. Petronio's communication privacy management (CPM) theory emphasizes how disclosing information is vital for building relationships, creating closeness, and creating intimacy. Thus, social isolation and loneliness resulting from under disclosure can be outcomes of privacy regulation gone wrong just as much as social crowding can be an issue. Similarly, the framework of contextual integrity explains that context-relative informational norms define privacy expectations and appropriate information flows and so a disclosure in one context (such as your doctor asking you for your personal medical details) may be perfectly appropriate in that context but not in another (such as your employer asking you for your personal medical details). Here it is not just about an information disclosure boundary but about a relationship boundary where the appropriate disclosure depends on the relationship between the discloser and the recipient. Drawing on Altman's theory of boundary regulation, Wisniewski et al. created a useful taxonomy detailing the various types of privacy boundaries that are relevant for managing one's privacy on social media. They identified five distinct privacy boundaries relevant to social media:

1. **Relationship:** This involves regulating who is in one's social network as well as appropriate interactions for each relationship type.

2. **Network:** This consists of regulating access to one's social connections as well as interactions between those connections.

3. Territorial: This has to do with regulating what content comes in for personal consumption and what is available in interactional spaces.

4. Disclosure: The literature commonly focuses on this aspect which consists of regulating what personal and co-owned information is disclosed to one's social network.

5. Interactional: This applies to regulating potential interaction with those within and outside of one's social network.

Of these boundary types, Wisniewski et al. emphasize the most important is maintaining relationship boundaries between people. Similarly, Child and Petronio note that "one of the most obvious issues emerging from the impact of social network site use is the challenge of drawing boundary lines that denote where relationships begin and end". Making sure that social media facilitates behavior appropriate to each of the user's relationships is a major challenge. Each of these interpersonal boundaries can be further classified into regulation of more fine-grained dimensions. Self- and Confidant Disclosures The information disclosure concerns described in the previous "Privacy Challenges" section are the focus of privacy around disclosure boundaries. Posting norms on social media platforms often encourage the disclosure of one's personal information (e.g., age, sexual orientation, location, personal images). Disclosing such information can leave one open to financial, personal, and professional risks such as identity theft. However, there are motivations for disclosing personal information. For example, research suggests that posting behaviors on social media platforms have a significant relationship with a desire for positive self-presentation. Privacy management is necessary for balancing the benefits of disclosure and its associated risks.

6.5 Addressing Privacy Challenges

Rather than just measuring privacy concerns, researchers and designers should focus on understanding attitudes towards boundary regulation. Validated tools for measuring boundary preservation concern and boundary enhancement expectations are provided in this chapter.

Privacy features need to be designed to account for individual differences in how they are perceived and used. While some feel features like untag, unfriend, and delete are useful, others are worried about how using such features will impact their relationships.

Unaddressed privacy concerns can serve as a barrier to using social media. It is crucial to design for not only functional privacy concerns (e.g., being overloaded by information, guarding from inappropriate data access) but social privacy concerns as well (e.g., unwelcome interactions, pressures surrounding appropriate self-presentation). This section describes how to better identify privacy concerns by measuring them from a boundary regulation perspective.We also emphasize the importance of individual differences when designing privacy features. Finally, we elaborate on a crucial set of social privacy issues that we feel are a priority to address. While many social media users may feel these types of social pressures to some degree, these problems have pushed some of society's most vulnerable to complete abandonment of social media despite their desire for social connection. We call on social media designers and researchers to focus on these problems which are a side effect of the technologies we have created.

6.6 Understanding People and Their Privacy Concerns

Understanding social media privacy as a boundary regulation allows us to better conceptualize people's attitudes and behaviors. It helps us anticipate their concerns and balance between too little or too much privacy. However, many existing tools for measuring privacy come from the information privacy perspective and focus on data collection by organizations, errors, secondary use, or technical control of data. In detailing the various types of privacy boundaries that are relevant for managing one's privacy on social media, Wisniewski et al. emphasized that the most important is maintaining relationship boundaries between people. similarly found that concerns about damaging relationship boundaries are actually at the root of low-level privacy concerns such as worrying about who sees what, being too accessible, or being bothered or bothering others by sharing too much information. For instance, a typically cited privacy concern such as being worried about a stranger knowing one's current location turns out to be a privacy concern only if an individual expects that a stranger might violate.

6.7 Measuring Privacy Concerns

Boundary regulation plays a key role in maintaining the right level of privacy on social media, but how do we evaluate whether a platform is adequately supporting it? A popular scale for testing users' awareness of secondary access is the Internet Users' Information Privacy Concerns (IUIPC) scale, which measures their perceptions of collection, control, and awareness of user data. An important finding is that users "want to know and have control over their information stored in marketers' databases." This indicates that social media should be designed such that people know where their data goes. However, throughout this chapter, it is evident that research on social media privacy has found concerns about social privacy more salient. In fact, the focus on relationship boundaries is a key privacy boundary to consider and measure in evaluating privacy concerns. Thus, having a scale to measure relationship boundary regulation would allow researchers and designers to better evaluate social media privacy.

For instance, Facebook, one of the most widely used platforms, was shown to both invoke high levels of concern as well as high levels of enhancement expectation. However, note that high frequency of use does not necessarily mean high levels of engagement (e.g., posting, commenting) or that users do not employ suboptimal workarounds (e.g., being vague in their posts). On the other hand, Twitter has a higher level of concerns compared to perceived enhancement and, accordingly, lower levels of usage.

6.8 Designing Privacy Features

When designing for privacy features, a crucial aspect to consider is individual differences. Privacy is not one-size-fits-all: there are many variations in how people feel, what they expect, and how they behave. Because social media connects individuals with diverse needs and expectations, and from a myriad of contexts, a necessity in addressing social media privacy is understanding individual differences in privacy attitudes and behaviors. Many individual differences have been identified that shape privacy needs and preferences and behaviors. Scholars have established that privacy as a construct is not limited to informational privacy (i.e., understanding the flow of data) but also includes social privacy concerns that may be more interactional (e.g., accessibility) or psychological in nature (e.g., self-presentation). Thus, a host of attitudes and experiences could shape an individual's view on what it means to have privacy online. For example, people's preferences for privacy tools could be heavily influenced by the type of data being shared or the recipient of that data. Likewise, prior experiences (negative or positive) could shape how people interact online which could affect disclosure. Context and relevance have also been found to significantly influence privacy behavior online. Drawing from the contextual integrity framework, many researchers argue that when people perceive data collection to be reasonable or appropriate, they are more likely to share information. On the other hand, research has shown that when faced with uncomfortable scenarios, people employ privacy protective behaviors such as nondisclosure or falsifying information. Research has also pointed to personal characteristics that could shape digital privacy behavior such as personality, culture, gender, age, and social norms.

While identifying concerns about damaging one's relationships is important to measure, understanding the individual differences that can lead someone to be concerned can provide insight into addressing these concerns. For instance, through a series of investigations, Page et al. uncovered a communication style that predicts concerns about preserving relationship boundaries on many different social media platforms. This communication style is characterized by wanting to put information out there so that the individual does not need to proactively inform others. Those who prefer an FYI (For Your Information) communication style are less concerned about relationship boundary preservation and, as a result, exhibit higher levels of engagement, interactions, and use of social media than low FYI communicators. For example, the survey items that capture an FYI communication style preference for location-sharing social media are: "I want the people I know to be aware of my location, without having to bother to tell them," "I would prefer to make my location available to the people I know, so that they can see it whenever they need it," and "The people I know should be able to get my location whenever they feel they need it." Each item is administered with a 7-point Likert scale (Disagree strongly, Disagree moderately, Disagree slightly, Neutral, Agree slightly, Agree moderately, Agree strongly). For other social media platforms, the information type is adjusted (i.e., "what I'm up to" instead of "my location").

Consequently, this raises concern over implications for non-FYI communicators since the design of major social media platforms is catered to FYI communicators. Drawing on this insight, Page demonstrated how considering the user's communication style when designing location-sharing socialmedia interfaces can alleviate boundary preservation concerns [129]. Certain design choices such as choosing a request-based location-sharing interaction can lower concerns fornon-FYI communicators, while continuous location-sharing and check-in type interactions that are typical in social media may be fine for FYI communicators.

This demonstrates that researchers should consider in the design of social media individual differences that affect privacy attitudes. Another individual difference in attitudes towards privacy features is a user's apprehension that using common features such as untag, delete, or unfriend/unfollow can act as a hindrance in their relationships with others. Page et al. identified that while many use privacy features and perceive them as a tool useful for protecting their privacy, there are also many who are concerned about how using privacy features could hurt their relationships with others (e.g., being worried about offending others by untagging or unfriending). Instead, those individuals would use alternative privacy management tactics such as vaguebooking (not sharing specific details and using vague posts). Designers need to be aware that privacy features also need to be catered to individual variations in attitudes as well or else they may be ineffective and unused by certain segments of the user population.

6.9 Privacy Concerns and Social Disenfranchisement

A significant amount of research within the domain of social media nonuse has been focused on functional barriers that hinder adoption. In many cases, nonuse is traced to a lack of access (e.g., limited access to technology, financial resources, or the Internet). However, the push against adoption and subsequent usage can be voluntary due to functional privacy concerns such as concerns about data breaches, information overload, or annoying posts [120]. Several social media companies have also implemented features such as time limits to help users counter overuse.

Likewise, it is equally important to consider social barriers that prevent social media engagement for people who really could use the social connection. Sharing about distressing experiences can be beneficial and reduce stigma, improve connection and interpersonal relationships with one’s network, and enhance well-being However, Page et al. identified a class of barriers that highlight social privacy concerns rooted in social anxiety or concerns about being overly influenced by others on social media. This is in contrast to the prior school of thought that focused primarily on functional motivations as barriers that influence nonuse. They point out that many who are already vulnerable avoid social media due to social barriers such as online harassment or paralysis over making decisions pertaining to online social interactions. Yet, they are also the ones who could benefit greatly from social connection and who end up losing touch with friends and social support by being off social media. They term this lose-lose situation of negative social consequences that arise when using social media as well as consequences from not using it, social disenfranchisement. They call on designers to address such social barriers and to realize that in designing the user experience to connect users so well, they are implicitly designing the nonuser experience of being left out. Given that social media usage may not always be a viable option, designers should design to alleviate the negative consequences of nonuse.

6.10 Guidelines for Designing Privacy-Sensitive Social Media

Now that you have learned about various privacy problems related to social media use, how do you apply that to designing or studying social media? Here are some practical guidelines.

Identifying Privacy Attitudes Measuring privacy attitudes is a tricky task. Using existing informational privacy scales, users often say they are concerned, but this does not end up matching their actual behavior. By approaching it from a boundary regulation perspective, it will be easier to identify the proper balance between sharing too much and sharing too little. The survey items described in this chapter offer a way to measure concerns about boundary regulation as well as positive expectations. Considering both are key to more accurately predicting user behaviors.

Understanding Your Target Population Some key characteristics are described in this chapter. Identifying these in your target population can help you be aware of individual differences that might affect privacy preferences on social media. When you are measuring privacy concerns, matching the preferences of your audience makes it more likely that they will have a good user experience. Pay particular attention to traits that have been identified as being related to usage and adoption of social media platforms, such as the FYI communication style which can be measured using the survey items provided in this chapter.

Evaluating Privacy Features Focus on understandingwhether users perceive your privacy features as useful or perhaps as posing a relational hindrance. The survey items provided in this chapter can help you do so. When anticipating privacy needs of your social media users, make sure you identify features that may impact boundary regulation both positively and negatively. You can compare attitudes between the existing feature and the newer version of the feature that will/has been deployed. You can also correlate attitudes towards privacy features with individual characteristics – some subpopulation of users may see privacy features as useful, while others may consider them a relational hindrance.

6.11 Check Your Progress

1. Explain how social media has transformed communication in the twenty-first century and discuss its impact on privacy.
2. What is the Privacy Paradox? Explain it with reference to privacy calculus and bounded rationality.

UNIT - 7

Privacy-Enhancing Technologies

Unit Structure

7.0 Objective

After completing this unit, students will be able to:

- Understand the concept and importance of privacy-enhancing technologies.

- Explain how secure messaging and end-to-end encryption protect communication.

- Identify privacy threats such as eavesdropping, MITM attacks, and data breaches.

- Describe the role of HTTPS and TLS in securing data transmission.

- Understand two-factor authentication and its importance in account security.

- Apply safe online practices to protect privacy and digital identity.

7.1 Introduction

An increasing amount of sensitive information is being communicated, stored, and shared online. Unauthorized access to this information can lead to serious privacy violations. This chapter focuses on some privacy-enhancing technologies (PETS) that prevent unauthorized access to sensitive information.

The need for effective privacy-enhancing technologies has never been greater. The Snowden revelations in 2013 exposed a broad array of government surveillance programs and ignited renewed interest in privacy-preserving technologies that prevent eavesdropping. The steady stream of data breaches underscores the risks of trusting third parties with sensitive information and the importance of robust defenses against unauthorized account access. Along with the risk of sensitive information disclosure, the rise of online social networks and other data-sharing cloud services presents increasing opportunities for privacy violations.

This chapter discusses several technologies that the usable security research community has analyzed and identifies issues, recommendations, and future research irections. For example, privacy-enhancing technologies protect sensitive information during transmission (HTTPS) and storage at untrusted third parties (end-to-end encryption in secure messaging and secure email). Technologies can also keep sensitive conversations private so that the fact that two parties are even communicating is not made public (Tor). Usable security researchers explore the human-computer interaction aspects of PETS, an important socio-technical element beyond the formal security guarantees established by a security analysis. A security technology that is not usable can lead to reduced security or no security at all.

7.2 Secure Messaging

Instant messaging (IM) applications provide an online chat capability that allows users to communicate in real time.Without end-to-end encryption, the conversation is not private. Early IM applications did not provide any encryption, allowing eavesdropping by the service provider or anyone with access to the network during transmission. For instance, other users on a wireless network with the proper software could easily view the chat messages.

IM applications typically rely on a centralized server to relay messages between the users. If each user connects to the server using HTTPS, no network eavesdroppers can read the messages. However, the service provider has access to the entire chat conversation when the server relays or stores the plaintext messages.

A significant post-Snowden development was the creation of the Signal Protocol by Moxie Marlinspike and Trevor Perrin. The protocol provides end-to-end encryption and is available inWhatsApp, the Signal app by OpenWhisper Systems, and Facebook Messenger Secret Conversations. Together, these applications serve over a billion users. Moxie and Trevor received the 2017 Levchin Prize for Real- World Cryptography for the development and widespread deployment of the Signal Protocol.

The widespread adoption and use of the Signal Protocol may represent the argest, most rapid adoption of end-to-end encryption in history. Interestingly, privacy was not a driving motivation for users to adopt these systems. Instead, adoption was based on the natural spread of messaging applications so that friends could communicate with their friends. The privacy benefits of encrypted conversations are a side benefit that did not drive adoption. Nonetheless, the result is that billions of users have private conversations protected against passive eavesdropping by the service provider, hackers, and governments without taking any action or even being aware of that protection.

With Signal, each user has a public and private key that the messaging app generates upon installation. Signal implementations rely on a server to relay messages and distribute public keys. When Alice and Bob want to communicate securely, they obtain each other's public key (sometimes referred to as their identity key) and jointly compute a shared key using their identity keys. As Alice and Bob exchange messages, they continue to calculate new shared keys to encrypt each message with a different encryption key. This approach provides forward secrecy, a significant privacy protection property in many state-of-the-art encryption systems.

Even if the encryption key for a message is compromised, the attacker gains access to only a single message and cannot read any previous or future messages using the compromised key.

All deployments of the Signal Protocol rely on a centralized key server trust model. The messaging provider maintains a key server that stores and hands out public keys for all users. Reliance on a trusted key server means that even though Signal protects against passive eavesdropping; users are vulnerable to an active man in-the-middle (MITM) attack.

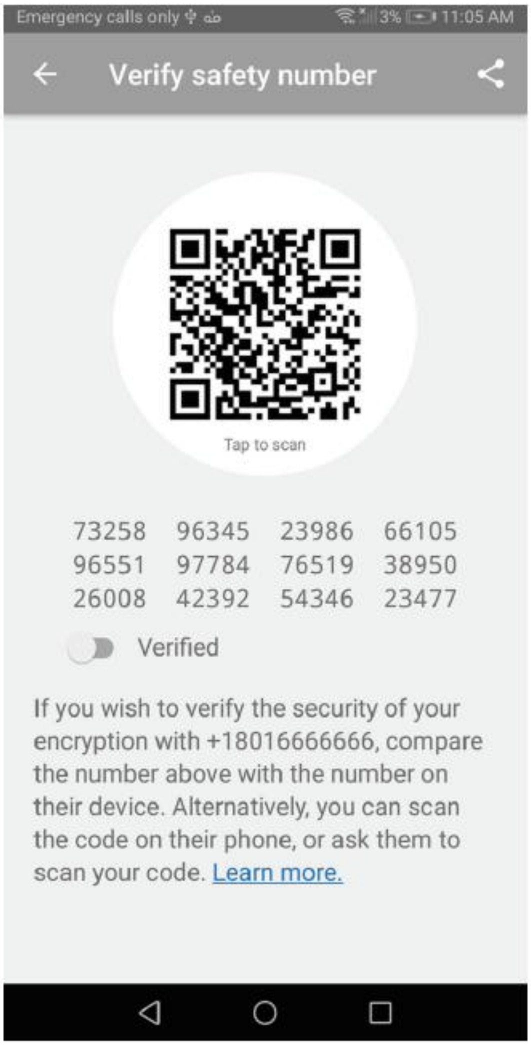
An active MITM attack works as follows. Suppose Alice and Bob want to have a private conversation. A compromised key server can hand out fake keys for Alice and Bob. As Alice and Bob send messages to each other, the compromised server can decrypt and possibly modify each message as it flows through the provider. Alice and Bob are not even aware that their messages are not private.

To defend against an active MITM attack, users can complete an authentication ceremony with each contact to verify out-of-band that their device has the correct public key of their contact and not a fake key from an active MITM attacker. Key verification requires that a pair of users each navigate to an interface in their messaging client and confirm that both users have the same fingerprint (sometimes called a safety number) on their phone as their partner. There are two ways to accomplish key verification. First, if the users are physically co-located, the app provides each with a QR code that they each scan from their partner’s phone to confirm that they have each other’s correct public key. The QR code confirmation requires that the partners meet and conduct the ceremony in person. If they areremote, they can confirm that they each have the same. One partner can read the safety number to the other partner to confirm. If the numbers match, the conversation is private. If the numbers don’t match, an active MITM attack is likely in progress.

The usable security research community has studied the effectiveness of the current authentication ceremony and proposed improvements based on usability study results. There have been studies that compare various methods for comparing fingerprints, along with studies that analyse the full authentication ceremony. More recently, a redesign of the authentication ceremony interface using opinionated design resulted in fewer mistakes and reduced the averagetime to find and complete the ceremony from 11 to 2 min.

XNext, an approach to automate the ceremony by confirming key ownership using social media accounts removed the requirement that both participants be physically present or communicate online while confirming each other’s keys. However, the results show that users do not trust social network providers as the third party to distribute their keys automatically.

XNext, an approach to automate the ceremony by confirming key ownership using social media accounts removed the requirement that both participants be physically present or communicate online while confirming each other’s keys. However, the results show that users do not trust social network providers as the third party to distribute their keys automatically.



73258 96345 23986 66105
96551 97784 76519 38950
26008 42392 54346 23477

If you wish to verify the security of your encryption with +18016666666, compare the number above with the number on their device. Alternatively, you can scan the code on their phone, or ask them to scan your code. Learn more.

7.3 Issues

Lack of user understanding—Users do not understand the need for the authentication ceremony to detect man-in-the-middle attacks.

Authentication ceremony is not usable—Lab studies show that the authentication ceremony is time-consuming, error-prone, and hard to use.

No interoperability—The current IM systems are walled gardens or silos. There is no interoperability between different providers. A WhatsApp user cannot communicate securely with a Facebook Messenger user.

Server must be trusted—The secure messaging provider is trusted to deliver public keys and provide the client software. Even if a user has the assurance that a contact's correct key is in use, there is still the risk that compromised software can leak keys or sensitive information. The government could still coerce a company to update the software on a target's phone with a backdoor.

7.4 Recommendations

Use secure messengers for private communication—For secure communication, the best option available today is for individuals to use an instant messenger client that supports the Signal Protocol for private conversations.

Vulnerable users should complete the authentication ceremony—If you are a high-risk target or are communicating highly sensitive data, complete the authentication ceremony with each contact to ensure there is no MITM attack.

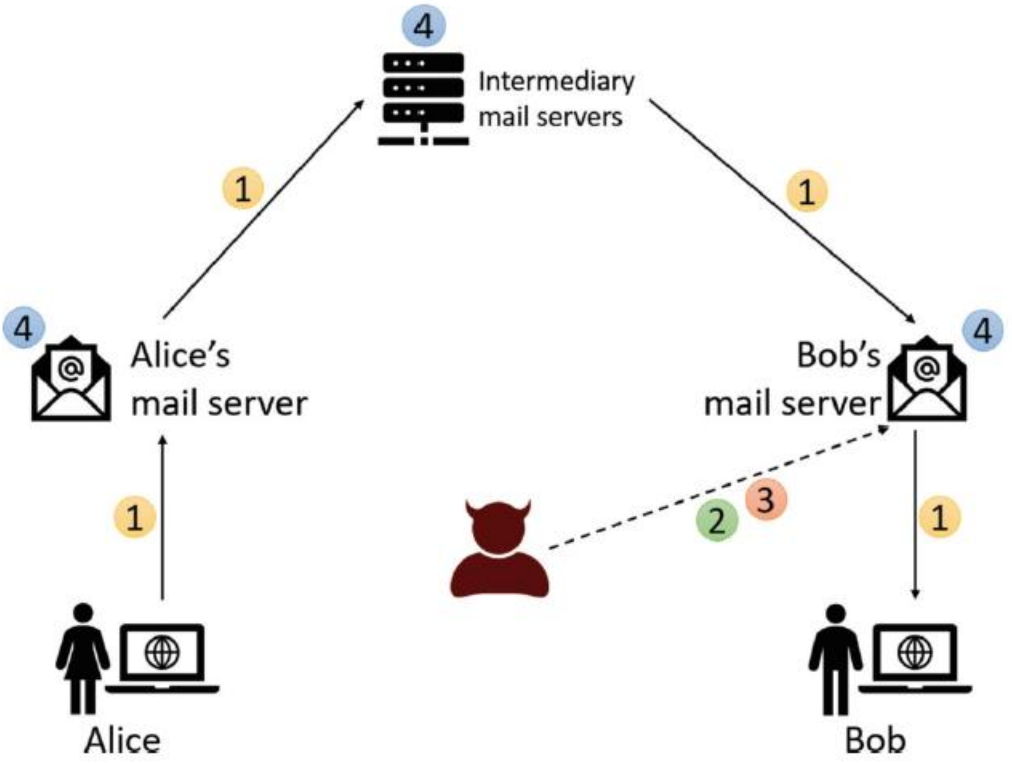
Automate key verification—Design methods to automatically detect or prevent active MITM attacks that relieve users from the burden of the authentication ceremony. Provide application-independent key management—Provide centralized support for key management in the browser or operating system to enable interoperability between applications that support the Signal Protocol. Better support for message deletion—Study user behavior and attitudes in response to new features that allow them to forget or delete messages.

Safeguard encryption keys—Design approaches utilizing secure enclaves to protect encryption keys and encryption software from compromise.

7.5 Secure Email

Email was not originally designed to be secure. Figure illustrates the vulnerabilities in plaintext email, including (1) unsecured links, (2) message forgeries, (3) malicious content, and (4) untrusted servers. Without the use of encryption, sensitive email messages are vulnerable to eavesdroppers while in transit. In addition, sensitive messages stored in the server are also vulnerable to unauthorized access.

Email messages are often stored indefinitely, and the long-term storage adds to the privacy risks even if the data is compromised well into the future. Technologies exist to address some of these vulnerabilities. Transport Layer ecurity (TLS) encrypts email messages during transmission between communication links. Sender Policy Framework (SPF) lets the domain owner specify the legitimate servers that send email messages for that domain. DomainKeys Identified Mail (DKIM) includes a signature on each email message from a domain to guard against message forgery. Recent studies show that these techniques are not universally deployed, leaving a significant gap in the secure email infrastructure. Even if we close this gap, servers still have access to plaintext email messages, and the threat of disclosure to hackers or government surveillance remains.



End-to-end encryption addresses the issue of server access to plaintext email. The most well-known secure email systems are S/MIME and PGP. S/MIME supports a hierarchical, top-down trustmodel and is used mainly in corporations. PGP supports a grass-roots, bottom-up trust model that is suitable for individuals. Deployment of these technologies continues to languish after decades. The reasons are complex and nuanced, and center around a diverse set of stakeholders with competing interests that no one-size-fits-all solution can satisfy.

Secure email is one of the challenges that launched the field of usable security with the seminal paper Why Johnny Can't Encrypt. The paper included a lab usability study of PGP that failed miserably and provided a wake-up call to the security community of the importance of user-centered design. Nearly 20 years later, a lab usability study of a modern PGP web client (Mailvelope) had similarly disappointing results when 9 of 10 participant pairs were unable to exchange a secure email message after 1 h of trying to use the system.

Despite the lack of a usable production PGP tool, recent research has produced several highly usable secure email interfaces. Figure illustrates the interface for Private Webmail 2.0, a system that grew out of a series of studies over many years. The research shows that the following are essential properties for a usable, secure email interface.

Tight Integration. Users want secure email systems that enhance their existing email clients and fit within their existing workflows. This integration is both visual and functional—that is, it looks like a part of the client application and has similar functionality, While visual integration is important, users should be able to clearly distinguish between emails protected with end-to-end encryption and emails that are not.

While most users prefer integrated solutions, a small but consistent portion prefer standalone clients, believing that handling secure email in a separate client makes it more obvious to the user when encryption is in use.

Inline, context-sensitive tutorials. Tutorials are essential in helping users understand how to use secure email properly. For users to pay attention and use these tutorials, the tutorial must be shown inline with the secure email system. Additionally, the system should provide context-sensitive tutorials, walking first-time users through the process of sending and receiving secure email.

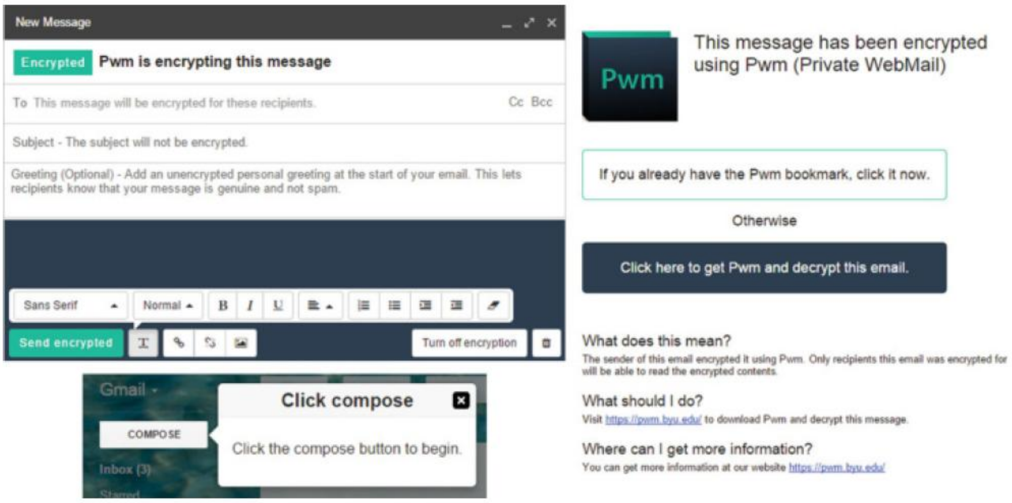
Streamlined onboarding. Encrypted email should be designed to help recipients understand what they have received and what actions they need to take next. If the secure email system requires recipients first to generate a key pair, the system should automatically send an email explaining what the recipient needs to do. Additionally, the system should save a draft of the sender's message to send automatically after the recipient generates and makes their public key available.

Understandable and trustworthy design. Interfaces need to help users understand how secure email is protecting them—for example, telling them whether the subject line is encrypted (it usually is not). Increased understanding allows users to make informed decisions and avoid mistakes. Additionally, system operation needs to conform to user expectations; otherwise, users reject the system. For example, studies show that if encryption happens too quickly, users assume that their messages were not encrypted and did not trust the tool.

Easy-to-use key management. Users struggle with managing their keys. Automation of key generation, uploading, and discovery significantly improve the user experience.

Studies show that systems applying (most of) these principles are perceived as highly usable, result in a low mistake rate, and help novice users begin sending encrypted email without expert assistance.

Secure email is a two-body problem, pioneered a novel two-person methodology where pairs of participants are brought into a user study to test a system. They found that participants were more relaxed during the study and



New Message
Encrypted
Pwm is encrypting this message
Cc Bcc
Sans Serif
Normal
B
I
U
Send encrypted
Turn off encryption
Gmail
COMPOSE
Inbox (3)
Starred
Pwm
If you already have the Pwm bookmark, click it now.
Otherwise
Click here to get Pwm and decrypt this email.

To This message will be encrypted for these recipients.

Subject - The subject will not be encrypted.

Greeting (Optional) - Add an unencrypted personal greeting at the start of your email. This lets recipients know that your message is genuine and not spam.

Click compose

Click the compose button to begin.

This message has been encrypted using Pwm (Private WebMail)

What does this mean?

The sender of this email encrypted it using Pwm. Only recipients this email was encrypted for will be able to read the encrypted contents.

What should I do?

Visit https://pwm.byu.edu/ to download Pwm and decrypt this message.

Where can I get more information?

You can get more information at our website https://pwm.byu.edu/

Top left—placeholder text that acts as an inline tutorial instructing users about how secure email works. Bottom left—an inline, context-sensitive tutorial helping users send an encrypted email for the first time.

Right—the body of the encrypted email providing plaintext instructions to streamline onboarding. Interface for private webmail (Pwm) 2.0, a modern usable secure email system did not automatically assume that they were responsible for system mistakes.

The storage of plaintext email at the server presents an attack surface in case of future account compromise. Research is beginning to explore email deletion capabilities that reduce the risk of future disclosure of sensitive messages that do not require long-term storage. Another approach is to encrypt the plaintext email on the server with a locally stored encryption key and delete the plaintext copy. The advantage of this approach is that a user can do this unilaterally without the cooperation of their communication partner. However, it does not safeguard the copy of the message in the original sender's outbox.

Multiple stakeholders with competing priorities for secure email make it difficult for a one-size-fits-all solution. There needs to be more willingness by the various stakeholders to allow for alternatives that support the needs of only some of the stakeholders. There has been significant effort by the usable security research community to study the issues surrounding secure email, and usable system designs have been demonstrated in a laboratory setting.

Issues

PGP is dead—PGP is a failed experiment. Even the proponents of secure email have been abandoning PGP recently. Modern PGP clients exhibit poor usability in laboratory user studies.

Secure email solutions are not interoperable—The various approaches to secure email are not interoperable (PGP, S/MIME, proprietary web-based systems).

It is difficult to introduce a secure email solution that maintains ubiquity—Email has a history emphasizing ubiquity and interoperability. Anyone can send an email to any other user if they have an email address for them. It is challenging to introduce secure email into this environment and maintain the same service guarantees.

7.6 Recommendations

Individuals should use secure messaging instead—Given the current state of secure email, use a secure messaging client that supports the Signal Protocol for private conversations with friends and family.

Businesses should use S/MIME or secure webmail—For sensitive business communications that must occur over email, enterprises can use S/MIME, and small businesses and individuals can use web-based secure email services such as ProtonMail and Tutanota.

All email providers should support TLS—It is exasperating that all email is not protected from passive eavesdropping today. All email systems should support TLS for exchanging email between email systems.

Delete old sensitive email when possible—Unless legally required to retain a copy, delete outdated sensitive email messages that could be problematic if made public following an account compromise.

Longitudinal studies are needed—Previous secure email usability studies are all short-term lab studies. Longitudinal studies could confirm whether the above design principles are sufficient for email or whether more improvements are needed to support long-term usage.

Providers should only have access to encrypted messages—Develop techniques to process encrypted data so the email provider can scan for malware and spam without having access to the plaintext.

Support easy deletion of old messages—Analyze the usability of secure email deletion approaches.

7.7 HTTPS

The privacy of sensitive information is protected when it is encrypted during transmission over an insecure network. HTTPS is the protocol for encrypting data transmitted between browsers and web servers. It relies on a lower-level protocol known as Transport Layer Security (TLS), formerly known as the Secure Socket Layer (SSL). At a high level, HTTPS/TLS/SSL are synonymous—it is the most common protocol for encrypted communication on the Internet. As part of the HTTPS setup, a website authenticates to the browser using a certificate digitally signed by a trusted third party.

In 2010, the Firesheep browser extension demonstrated the risks of session hijacking for sites that used HTTPS only to protect the login page and sent browser cookies in the clear. The tool allowed an attacker sniffing traffic on a wireless network to easily hijack another user's session to gain unauthorized access to their social network or webmail. The publicity and ease of performing this attack contributed to major websites, like Google and Facebook, requiring HTTPS for all session traffic to their website.

More recently, there has been a significant uptick in the use of HTTPS for all web traffic, which provides increased protection against unauthorized access to browser activity. The increase in HTTPS has been mainly fueled by Let's Encrypt, a service that offers free digital certificates that are easy for admins to request and manage.

The most recent version of the protocol (TLS 1.3) supports only ciphers that provide the forward secrecy property described earlier in the secure messagingdiscussion. It also provides increased privacy protection by encrypting the server certificates transmitted to the client. There are three aspects of HTTPS that have socio-technical implications: (1) TTPS warning messages, (2) developer and administrator development and deployment hurdles, and (3) HTTPS inspection.

7.8 HTTPS Warning Messages

Users are sometimes faced with HTTPS warning messages when the browser encounters a website certificate that does not properly validate. The web servercertificate authenticates a website to the browser. HTTPS warnings have been an area of significant usability studies and modification over the past decade. Researchers at Google have been at the forefront of this effort. Google is well-positioned to gather telemetry data from its users and conduct large-scale A/B tests comparing alternate designs. The results of these studies have shown a decrease in the click-through rate of HTTPS warning messages. It isn't clear that the reduction is due to increased user understanding as much as it is that the browsers make it more difficult to click through the warning message by adding additional steps that may discourage users from continuing.

Browsers display a lock icon whenever HTTPS is in use. Users interpret the lock icon as an indicator that the website is secure. Several studies show that users interpret the lock icon to mean that the website is secure. The lock icon is unrelated to the website’s security, and this misunderstanding is precisely the wrong interpretation when a phishing website impersonates a well-known company and employs HTTPS.

7.9 HTTPS Development and Deployment

Software developers that build HTTPS applications can make mistakes, such as introducing certificate validation errors that compromise user privacy. Two recent research projects presented user-level and system-level approaches for automatically intercepting and verifying a website certificate, which overrides an application with broken HTTPS authentication. An approach that goes beyond intercepting brokenHTTPS applications is to design amore straightforward, abstract interface to HTTPS applications that make it easier for developers to build reliable applications that encrypt network traffic. a simple extension to the existing POSIX secure socket API.

Administrators of websites can misconfigure HTTPS and create privacy risks for users. A qualitative study examined mental models of users and administrators, and administrators did not understand protocol components and technical terms associated with HTTPS.

7.10 HTTPS Interception

HTTPS interception (also known as a TLS Proxy) often occurs within a corporation, library, or school so that the organization can monitor the security of their network and make sure clients are not unknowingly downloading malware or releasing sensitive business secrets from a compromised machine. Several studies measure how often HTTPS inspection occurs by using detection techniques from the server side. A study of client-side HTTPS interception software shows that these systems can introduce privacy risks to users due to programmer error.

The same mechanisms utilized for inspection can also be the source of an active man-in-the-middle attack. Since the two options appear similar, it makes the task of informing the user all the more difficult.

7.11 Issues

Companies perform HTTPS Interception to protect their network and systems. Intermediate servers run by a company or organization can access a user's HTTPS web traffic, known as HTTPS inspection. Some users consider this a privacy breach, but they understand why a company must protect its network.

Users overwhelmingly desire notification when an HTTPS proxy is operating.

Many HTTPS applications are broken. Developers make mistakes when building HTTPS applications due to the complexity of HTTPS libraries.

7.12 Recommendations

Use HTTPS on all websites. All owners of websites should be using HTTPS for all connections to their site. Certificates are inexpensive and easy to acquire using Let's Encrypt.

Website designers should not mix HTTP and HTTPS traffic on a single web page since this has been a source of compromise in the past.

7.13 Check Your Progress

1. Describe secure messaging and explain how end-to-end encryption and the Signal Protocol protect user privacy.
2. What is a Man-in-the-Middle (MITM) attack in secure messaging? Explain the authentication ceremony used to prevent it and its limitations.
3. Discuss the major issues and recommendations related to secure email, highlighting why secure email adoption remains challenging.
4. Explain HTTPS and its role in protecting data during transmission. Discuss the usability issues related to HTTPS warning messages.
5. What is Two-Factor Authentication (2FA)? Explain its importance, common usability issues, and recommendations for improving user adoption.

UNIT- 8
Privacy and Security in Social Media

8.1 OBJECTIVES

After completing this unit, students will be able to:

- Understand the concept of privacy and security in social media and their importance in daily digital life.
- Explain the meaning of privacy and security in social media platforms with suitable examples.
- Identify various privacy issues and security threats associated with social media usage.
- Analyse the importance of protecting personal information from misuse, cybercrime, and identity theft.
- Describe different ways and best practices to protect privacy and security on social media platforms.
- Develop safe and responsible online behaviour for effective and secure use of social media.

8.2 INTRODUCTION

Social media has become an essential part of modern life, allowing people to communicate, share information, and build communities across the world. Platforms such as social networking sites, messaging apps, and content-sharing services make it easy to connect with others instantly. However, along with these benefits come serious concerns about privacy and security. Users often share large amounts of personal information online, which can be misused if not properly protected. Understanding privacy and security in social media is important to ensure safe and responsible use of these platforms.

8.3 MEANING OF PRIVACY IN SOCIAL MEDIA

Privacy in social media refers to the protection of users' personal information, such as names, photos, locations, contact details, and personal opinions. It also includes controlling who can see, share, or use this information. Many users are unaware that their data may be collected, stored, and sometimes shared with third parties without explicit consent.

Why Privacy Matters

Social media platforms like Facebook, Instagram, Twitter (now X), and TikTok thrive on user-generated content, but this comes at the cost of privacy. Every like, comment, share, or post creates a digital footprint that platforms analyze using algorithms. This data fuels targeted advertising, but it can also lead to misuse, such as identity theft, stalking, or discrimination. For instance, in 2018, the Cambridge Analytica scandal revealed how Facebook data from 87 million users was harvested to influence elections, highlighting how "free" services monetize personal info.

Common Privacy Risks

Data Collection: Platforms track not just what you post, but also your browsing habits, device info, and even microphone/camera access via apps.

Third-Party Sharing: Apps and advertisers access your data through APIs; a simple quiz app might pull your friend list and location.

Cyber Threats: Hackers exploit weak privacy settings for phishing, doxxing (publicly exposing private info), or ransomware.

Government Surveillance: In countries like India, laws like the IT Rules 2021 require platforms to trace user data, balancing security with privacy erosion.

How Platforms Handle Privacy

Most sites offer privacy settings—like "friends only" posts or two-factor authentication—but defaults are often public to boost engagement. Features like Stories (temporary posts) or end-to-end encryption in WhatsApp help, yet metadata (e.g., who you message) remains visible. Regulations like GDPR in Europe or India's DPDP Act 2023 aim to enforce consent and data minimization, giving users rights to delete or port their data.

Tips for Protecting Your Privacy

Adjust settings: Make profiles private, limit app permissions, and review tagged photos.

Use tools: Enable VPNs, incognito mode, or privacy-focused apps like Signal.

Be mindful: Avoid oversharing; think "Would I say this in public?"

Stay informed: Regularly update apps and read privacy policies (short versions exist on most sites).

Ultimately, true privacy requires user vigilance alongside better platform accountability. In an interconnected world, safeguarding your digital self prevents real-world harm.

8.4 MEANING OF SECURITY IN SOCIAL MEDIA

Security in social media involves protecting accounts and data from unauthorized access, cyberattacks, hacking, identity theft, and online fraud. Strong security measures help prevent criminals from misusing user accounts or stealing sensitive information, ensuring users can interact safely without fear of exploitation.

Why Security Matters

Social media is a prime target for cybercriminals due to its vast user base—over 5 billion globally, including 500+ million in India. Weak security doesn't just risk personal data; it enables scams like fake giveaways or phishing that spread malware. High-profile breaches, such as the 2021 Facebook hack affecting 533 million users (including leaked Indian phone numbers), show how one vulnerability cascades into mass harm.

Common Security Threats

Phishing Attacks: Fake login pages trick users into entering credentials.

Account Takeovers: Password stuffing (reusing stolen passwords) or SIM-swapping to hijack 2FA.

Malware and Ransomware: Malicious links in DMs encrypt devices for ransom.

Social Engineering: Scammers pose as friends to extract info or money.

DDoS Attacks: Overloading platforms to disrupt services, as seen in assaults on Twitter.

Key Security Mechanisms

Platforms deploy layered defenses:

Authentication: Multi-factor authentication (MFA), biometrics, and passwordless logins.

Encryption: HTTPS for data in transit; end-to-end for messages (e.g., WhatsApp).

AI Monitoring: Algorithms detect suspicious logins from new devices or locations.

Compliance: Adhering to standards like ISO 27001 or India's CERT-In guidelines for breach reporting within 6 hours.

Best Practices for Users

- Use strong, unique passwords managed by tools like password managers (e.g., Bitwarden).
- Enable MFA everywhere and avoid SMS-based (opt for app authenticators).
- Verify links before clicking; report suspicious activity promptly.
- Keep apps updated and use antivirus software.
- Limit third-party app access via settings.

In essence, social media security is a shared responsibility—platforms provide tools, but users must adopt them proactively to counter evolving threats.

8.5 PRIVACY ISSUE IN SOCIAL MEDIA

Oversharing of personal information: Users post details like home addresses, phone numbers, or routines (e.g., "Live from my favorite café!"), inviting stalkers or burglars.

Data collection without user awareness: Platforms harvest metadata like IP addresses, contacts, and browsing history via cookies and trackers, often buried in lengthy terms of service.

Tracking of user activities: "Like" buttons and pixels on external sites follow you across the web, building detailed profiles sold to advertisers.

Misuse of personal photos and videos: Images can be deepfaked, revenge-porned, or used in catfishing scams without consent.

Lack of control over shared content: Once posted, content can be screenshotted, shared indefinitely, or algorithmically amplified beyond your network.

These issues can lead to loss of privacy, reputation damage, emotional stress, identity theft, or even physical harm—like the 2014 case of a Delhi teen stalked via Instagram geotags.

8.6 SECURITY THREATS

Social media users face several security threats, such as:

Hacking and account takeover: Cybercriminals use credential stuffing or brute-force attacks to seize control, then post spam or demand ransom (e.g., 2022 Twitter hack of high-profile accounts).

Phishing attacks and fake links: Deceptive messages mimic friends or brands, tricking users into fake login pages (e.g., "Your account is suspended—click here").

Malware and spyware: Infected links or apps install keyloggers to steal data; mobile malware rose 30% in India in 2025 per CERT-In.

Identity theft: Stolen profiles enable impersonation for scams or reputational harm.

Online scams and fraud: Fake giveaways, romance scams, or job offers extract money—India lost ₹1,200 crore to such frauds in 2024.

Weak passwords and careless clicking often increase these risks, amplifying vulnerabilities in platforms handling billions of daily interactions.

Additional Security Threats

SIM Swapping: Attackers hijack phone numbers to bypass 2FA, accessing linked accounts.

DDoS Attacks: Flood platforms to crash services, enabling theft during chaos.

Social Engineering: Manipulating users via DMs to reveal info (e.g., "Send OTP for verification").

Ransomware: Locks devices after clicking malicious ads, demanding crypto payment.

Man-in-the-Middle (MitM) Attacks: Intercept unencrypted Wi-Fi data on public networks.

8.5 IMPORTANCE OF PRIVACY AND SECURITY

Protecting privacy and security on social media is important because it:

Safeguards personal and financial information: Prevents leaks of addresses, bank details, or health data that could lead to fraud.

Prevents cybercrimes and online harassment: Stops hacking, doxxing, or bullying that affects mental health—1 in 5 Indian teens report cyberbullying per NCRB 2025.

Maintains user trust and safety: Builds confidence in platforms, encouraging positive engagement without fear.

Protects individuals from identity theft and misuse of data: Blocks scammers from impersonating you or selling profiles on dark web markets.

Additional Key Reasons

Preserves Reputation and Career: Old posts can resurface, costing jobs (e.g., 2024 cases of influencers blacklisted over leaked data).

Supports Mental Well-Being: Reduces anxiety from constant surveillance or unwanted exposure.

Enables Regulatory Compliance: Aligns with laws like India's DPDP Act 2023, avoiding fines up to ₹250 crore for platforms.

Fosters Innovation: Secure environments promote features like secure payments (e.g., Instagram Shopping) without breach fears.

National Security: Curbs misinformation or foreign interference, as seen in 2024 election hacks.

8.6 WAYS TO PROTECT PRIVACY AND SECURITY

Using strong and unique passwords: Combine letters, numbers, symbols (e.g., "Sm@rtAss@m2026!"); avoid "123456" or birthdays.

Enabling two-factor authentication (2FA): Adds a code from an app like Google Authenticator—blocks 99% of automated hacks.

Adjusting privacy settings: Switch to "friends only," disable search engine indexing, and review tagged content.

Avoiding suspicious links and messages: Hover to check URLs; use scanners like VirusTotal.

Limiting the sharing of personal information: Skip posting addresses, schools, or routines; use vague terms like "out and about."

Logging out from public devices: Clear cookies and use incognito mode on cyber cafés or shared PCs.

Privacy-Focused Actions

Regular Audits: Monthly check who sees your posts; delete inactive accounts.

Ephemeral Sharing: Use disappearing messages (e.g., WhatsApp) or Stories.

Data Minimization: Opt out of ad tracking via settings (e.g., "Off-Facebook Activity").

Security-Focused Actions

Software Updates: Enable auto-updates to patch vulnerabilities—critical after 2025 Log4j exploits.

Antivirus and VPNs: Install apps like Norton or ExpressVPN, especially on public Wi-Fi.

Device Security: Use biometric locks and encrypt phones.

Awareness and Reporting

Verify Before Engaging: Confirm friend requests; ignore unsolicited prizes.

Report Incidents: Use platform tools or India's National Cyber Crime portal (cybercrime.gov.in).

Educate Yourself: Follow CERT-In alerts and BAOU cybersecurity modules.

Tools and Resources Table

8.7 CHECK YOU PROGRESS

- Explain the meaning of privacy and security in social media with examples. Discuss common privacy issues like oversharing and data collection, and how they lead to real-world harm such as identity theft or stalking.

- Describe five major security threats in social media (e.g., phishing, malware, account takeover). Provide examples from India (like CERT-In reported incidents) and their consequences for users.

- Why is protecting privacy and security crucial on social media? Elaborate on benefits like preventing cybercrimes, maintaining trust, and compliance with laws such as India's DPDP Act 2023.

- Outline at least eight ways to protect privacy and security (e.g., strong passwords, 2FA, privacy settings). Explain how each works and recommend tools like Bitwarden or VPNs with step-by-step implementation.

- Differentiate between privacy risks (e.g., tracking, photo misuse) and security threats (e.g., hacking, scams). Suggest integrated measures for BAOU students using social media for education.

Fill in the Blanks

__________ authentication uses a second factor like an app code to secure accounts.
Answer: Two-factor (or 2FA)

Platforms collect user data via __________ and cookies without always informing users.
Answer: Tracking

__________ swapping hijacks phone numbers to bypass account security.
Answer: SIM

Always __________ out from public devices to prevent unauthorized access.
Answer: Log

India's __________ Act 2023 mandates consent for data processing in social media.
Answer: DPDP