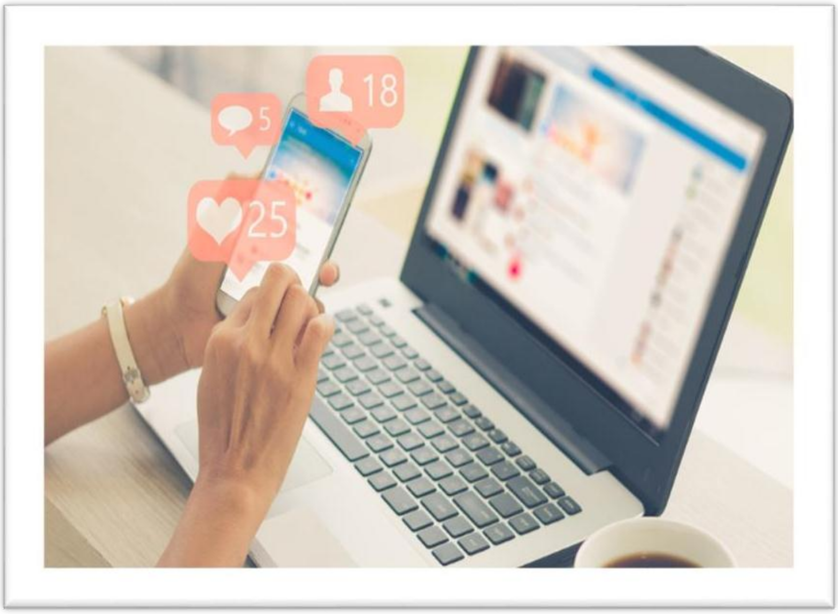
Scenario 1 : Posting Private information on Social Media



What Is Social Media

Social media facilitates the sharing of ideas and information through virtual networks. From Facebook and Instagram to Twitter and YouTube, social media covers a broad universe of apps and platforms that allow users to share content, interact online, and build communities. More than 4.7 billion people use social media, equal to roughly 60% of the world’s population.1

Today, social media messaging apps and platforms are the most commonly used sites worldwide. In early 2023, 94.8% of users accessed chat and messaging apps and websites, followed closely by social platforms, at 94.6% of users. Search engine sites were next, with 81.8% of users accessing them.

What Are the Types of Social Media

Social media platforms can be categorized according to the interests of their users and their purposes. There are platforms that appeal to video game players, social gamers, video sharers, professional business networks, virtual worlds, review platforms, and beyond.

People use various social media applications to network career opportunities, find others across the globe with like-minded interests, and share their political views. Entertainers and politicians use social media to engage with constituents and voters.

For businesses, social media has become a key tool. Companies use the platforms to find and engage with customers, drive sales through advertising and promotion, gauge consumer trends, and offer customer service or support.

Social media's ability to collect information helps businesses to fine-tune their marketing campaigns and conduct market research. It helps companies promote products and services as it enables the distribution of targeted, timely, and exclusive sales and coupons to potential customers. Further, social media can help build customer relationships through loyalty programs linked to social media.

How Did Social Media Evolve

Social media originated as a way to interact with friends and family but soon expanded to serve many purposes. In 2004, MySpace was the first network to reach one million monthly active users.3

Social media participation exploded in the years that followed with the entry of Facebook and Twitter. Businesses gravitated toward these platforms in order to reach an audience instantly on a global scale.

On average, global users spent 2.24 hours each day on social networks in 2020, the highest across almost any media type.2Global Web Index. "The Global Media Landscape."

According to Global Web Index, 46% of internet users worldwide get their news through social media platforms. That compares to 40% of users who view news on websites. Gen Z and Millennials were most likely to view news on social media sites versus other generations.2

What Are the Benefits of Social Media

Social media platforms allow people to access information in real-time, to connect, and to find niche communities. It has helped many individuals find common ground with others online, making the world seem more interconnected and within reach.

On the other hand, social media is prone to spreading disinformation, creating polarization, and even causing harmful psychological effects.

Still, according to a 2019 survey by Pew Research Center, people's use of social media is correlated with having more friends and more diverse personal networks, especially within emerging economies.For 80% of teenagers, social media allows them to feel more connected to peers, according to a 2022 Pew Research Center survey of U.S. teens ages 13 to 17. Overall, one in three said that social media has had a mostly positive effect on them, while 59% said it had neither a positive nor a negative effect.

Businesses are also using social media marketing to target their consumers, build a loyal fan base, and create a culture behind their brands. According to Facebook, more than 200 million small businesses use their platform for marketing purposes.

What Are the Top Social Media Sites

1. Facebook (2.96 billion users)
2. YouTube (2.51 billion users)
3. WhatsApp (2 billion users)
4. Instagram (2 billion users)
5. WeChat (1.31 billion users)
6. TikTok (1.05 billion users)
7. Facebook Messenger (931 million users)
8. Douyin (715 million users)
9. Telegram (700 million users)
10. Snapchat (635 million users)

Risks of Sharing Personal Identity on Social Media

1. Posting personal information on social media can expose you to various risks and negative consequences. Here are some reasons why you should be cautious about sharing personal information online:
2. Fraud A data leak can reveal everything from social security numbers to banking information. Once criminals have these details, they can engage in all kinds of scams on your behalf.
3. Financial Crime Personal identity theft in the form of a Population Identification Number (NIK), full name, and address can be used for financial crimes such as applying for bank loans, online loans, credit cards, illegal money transfers, tax fraud, and extortion.
4. Phishing Personal identity theft in the form of e-mail addresses and telephone numbers has the potential to be used to access online accounts, advertising spam through e-mail marketing, and telemarketing targets.

Things Not to Share on Social Media

1. Financial Data Sharing debit card information, credit, payslips, credit card numbers and CVV, moreover details about bank accounts must be confirmed because nowadays many hackers can easily break into.
2. Private documents Documents containing personal data including names such as Identity Cards, Driver's Licenses, passports and OTP codes must be kept.
3. Travel Ticket/Boarding Pass All personal data and order details are in one barcode. Data from Krebs on Security shows that a boarding pass can be said to be a treasure, because it contains the first and last name, flight number, and the date the boarding pass was printed.
4. Selfie while holding KTPAs you know, many financial services use selfie photos while holding an ID card as a condition for verifying identity and authenticating an account so that it cannot be shared on social media so as not to be misused.
5. Current location Be careful about sharing your current location, especially if you're in a quiet place alone. Your posts may invite crimes such as theft, robbery, or other criminal activities.
6. Digital identity Confidential digital identity containing e-mails, phone numbers, addresses and other personal information to prevent data hacking.

Tips for Maintaining Personal Identity Security on Social Media

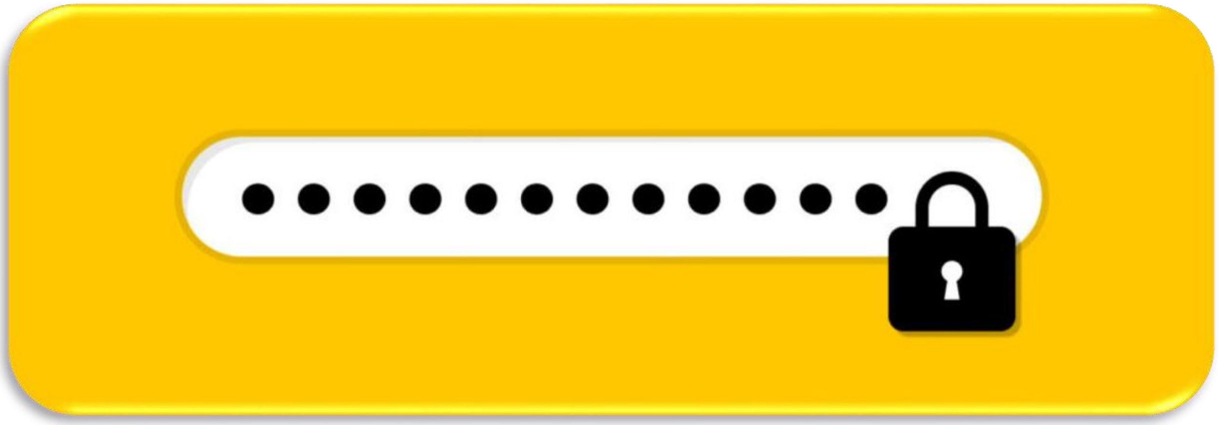
1. Change Password Use difficult social media passwords and different passwords for each social media account so that when one account is hacked, the other accounts are not easily hacked as well. Make sure you change your password regularly.
2. Keep Personal Information Confidential Avoid displaying personal information such as your mother's name, telephone number, ID card number, bank account number, and e-mail address to avoid misuse of data by irresponsible parties.
3. Be Careful in Opening Links Check the URL addresses of email attachments and visited sites so as not to enter fake sites that want to steal personal data.
4. Keep Other People's Personal Information Confidential Respect the privacy of others by not sharing personal information on social media without the person's permission.
5. Set Privacy Settings Set the privacy settings on your social media accounts to determine who can access your profile and posts.
6. Public Connection Alert Take care of your digital security by being careful not to share personal identities when using public connections as they are prone to hacking

Conclusion

In general, it's important to be cautious and mindful of what you share on social media platforms. Regularly review your privacy settings, limit the personal information you disclose, and think twice before posting anything that could have potential negative consequences in the future. It's always a good idea to maintain a healthy balance between sharing and protecting your personal information online.

Scenario 2 : What password you choose when creating new account for Social Media

What is Password



A password is a secret combination of characters, typically used to authenticate and verify the identity of a user before granting access to a system, application, account, or device. Passwords are a fundamental aspect of online security and are used to protect sensitive information from unauthorized access.

Passwords can take the form of a sequence of letters, numbers, and special characters. They serve as a barrier to prevent unauthorized users from gaining access to personal or confidential data. When creating a password, it's important to make it strong and unique to enhance security.

There are two main types of Passwords

1. Weak password
2. Strong password

What are strong and weak passwords

A strong password : is a combination of characters that is difficult to guess or crack, providing a high level of security for your accounts and sensitive information. In contrast, a weak password is easily guessable or can be compromised relatively easily, putting your accounts and data at risk.

A weak password : is a password that lacks sufficient complexity and security, making it easily guessable or susceptible to being compromised by attackers. Weak passwords are often short, simple, and follow predictable patterns, which makes them vulnerable to various forms of cyberattacks

Comparision between Weak password, Better password and Strong password

Weak Password	Better Password	Strong Password
kitty	1Kitty	1Ki77y
susan	Susan53	.Susan53
jellyfish	jelly22fish	jelly22fi$h
smellycat	sm3llycat	$m3llycat
allblacks	a11Blacks	a11Black$
usher	!usher	!ush3r
ebay44	ebay.44	&ebay.44
deltagamma	deltagamm@	d3ltagamm@
ilovemypiano	!LoveMyPiano	!Lov3MyPiano
Sterling	SterlingGmal2015	SterlingGmail20.15
BankLogin	BankLogin13	BankLogin!3

Steps for creating a strong and secure password when signing up for a new social media account

1. **Length:** Use a password that is at least 12 characters long. Longer passwords are generally more secure.
2. **Complexity:** Include a mix of uppercase and lowercase letters, numbers, and special characters (such as !, @, #, $, etc.).
3. **Avoid Dictionary Words:** Don't use easily guessable words, names, or phrases that can be found in the dictionary or are related to you (like "password," "123456," your name, or "admin").
4. **Randomness:** Create a password that appears random and isn't based on easily discoverable information (like your birthday or a common pattern).
5. **No Personal Information:** Avoid using easily accessible personal information, such as your birthdate, phone number, or address.
6. **Unpredictability:** Use a combination of characters that doesn't follow a predictable pattern.
7. **Passphrases:** Consider using a passphrase—a series of random words or a sentence that is

Conclusion

Remember that the goal is to create a password that is difficult for others to guess or crack while being manageable for you to remember or securely store. By following these guidelines, you can help protect your social media accounts from unauthorized access and potential security breaches

Scenario 3 : Using Public WI-FI.

What is WI-FI

- Wi-Fi, short for "Wireless Fidelity," is a technology that allows electronic devices to connect to the internet or communicate with each other wirelessly using radio waves. It enables devices like smartphones, laptops, tablets, smart TVs, and more to connect to the internet and local area networks (LANs) without the need for physical cables.
- Wi-Fi networks are created using a wireless router, which serves as a central hub for connecting devices. The router connects to the internet via a wired connection (such as a DSL or cable modem) and then broadcasts a wireless signal that devices can detect and connect to. To connect to a Wi-Fi network, you need a compatible device (such as a smartphone or laptop) with Wi-Fi capabilities. Once connected, your device can access the internet, local network resources, and other devices on the same network.
- Each Wi-Fi network has a unique name called the SSID, which you select when connecting a device. Password protection, in the form of a WPA or WEP key, is often used to secure these networks.Wi-Fi operates on different frequency bands, such as 2.4 GHz and 5 GHz, each with its own advantages in terms of range and data transfer rates.
- To protect data transmitted over Wi-Fi from unauthorized access, encryption protocols like WPA and WPA2/WPA3 are commonly employed for security.
- Public places often offer Wi-Fi hotspots, allowing visitors to connect to the internet with their devices, making Wi-Fi a ubiquitous technology in modern society.

Public and Private WIFI.

Public Wi-Fi

Public Wi-Fi is a wireless network that is made available for use by the general public in places like cafes, airports, hotels, libraries, shopping malls, and other public spaces. These networks are typically provided by businesses or organizations to offer internet access to their customers, visitors, or passersby. Public Wi-Fi networks are open and do not require a password to connect. They are meant to be convenient for users who want to access the internet on their devices while in a specific location.

However, public Wi-Fi networks come with certain security risks. Since they are open and accessible to anyone in the vicinity, they can be more vulnerable to cyberattacks, such as data interception, hacking, and identity theft. Malicious actors can potentially eavesdrop on the data being transmitted over these networks, particularly if the connection is not encrypted or secured properly.

Private Wi-Fi

Private Wi-Fi refers to a wireless network that is set up within a specific location, such as a home, office, or business. Private Wi-Fi networks are secured with a password and encryption to prevent unauthorized access. Only individuals who have the correct password can connect to the network. Private Wi-Fi networks offer more control over who can access the network and provide a higher level of security compared to public Wi-Fi networks.

Private Wi-Fi networks are commonly used for internal communication, sharing resources within a local area network, and accessing the internet within a specific location. These networks are less susceptible to eavesdropping and unauthorized access because of the security measures in place.

Risk of using public Wi-fi.

Public Wi-Fi can be dangerous due to its open nature and the lack of security features that are often present in private networks.

Some reasons why public Wi-Fi can pose risks:

1. Lack of Encryption: Many public Wi-Fi networks do not have proper encryption in place to protect the data being transmitted between devices and the network. This means that data sent over these networks can be intercepted by malicious actors who are within range of the network. This could include sensitive information like login credentials, personal messages, and financial details.
2. Man-in-the-Middle Attacks: Cybercriminals can set up fake Wi-Fi hotspots with names similar to legitimate networks. When users unknowingly connect to these fake networks, attackers can intercept and manipulate the data being exchanged between the user and the internet. This is known as a man-in-the-middle (MITM) attack.
3. Unencrypted Websites: Even if a public Wi-Fi network uses encryption for its connection, if the websites you visit are not using HTTPS (secure HTTP), the data you exchange with those sites is still vulnerable to interception. Attackers can potentially capture sensitive information from unencrypted connections.
4. Rogue Hotspots: Malicious actors can set up their own Wi-Fi hotspots in public places, mimicking legitimate networks. Unsuspecting users might connect to these rogue hotspots, enabling attackers to monitor their online activities and potentially inject malicious content.
5. Malware Distribution: Public Wi-Fi networks can serve as platforms for distributing malware. Malicious software can be injected into the data traffic passing through the network, infecting users' devices when they connect.

How to Safely use Public Wi-Fi.

Safely using public Wi-Fi involves taking precautions to protect your personal and sensitive information from potential security risks.

Some steps you can take to use public Wi-Fi more securely:

1. Use a Virtual Private Network (VPN): A VPN encrypts your internet traffic and routes it through a secure server, making it much more difficult for hackers to intercept your data. Before connecting to a public Wi-Fi network, consider using a reputable VPN service to ensure your online activities remain private.
2. Update Your Device: Make sure your device's operating system, apps, and security software are up to date. Updates often include security patches that help protect against known vulnerabilities.
3. Turn Off Sharing: Disable file and printer sharing, as well as public folder sharing, on your device to prevent unauthorized access to your files and folders.
4. Enable Firewall: Activate your device's firewall to add an extra layer of protection against unauthorized incoming connections.
5. Forget Networks: After using a public Wi-Fi network, ensure your device doesn't automatically connect to it in the future. "Forget" the network so you have control over when you connect.
6. Avoid Sensitive Activities: Refrain from accessing sensitive information such as online banking, shopping with credit cards, or entering personal credentials on public networks. If you

need to perform such activities, consider using your cellular data connection or a trusted network.

How Public Wi-Fi can be Hacked.

Public Wi-Fi can be hacked through various methods due to its open and unsecured nature. Some common techniques that hackers might use to compromise public Wi-Fi networks and the devices connected to them:

1. Man-in-the-Middle (MITM) Attacks: Hackers can intercept the communication between your device and the public Wi-Fi network. They position themselves between your device and the network, capturing the data you send and receive. This allows them to potentially steal sensitive information like login credentials, credit card numbers, and personal messages.
2. Rogue Hotspots: Attackers can set up fake Wi-Fi hotspots with names similar to legitimate networks. Unsuspecting users might connect to these rogue networks, giving hackers access to their data. This is especially effective in high-traffic areas where users are eager to connect quickly.
3. Evil Twin Attacks: Similar to rogue hotspots, attackers create a malicious duplicate of a legitimate Wi-Fi network. Users unknowingly connect to the evil twin, allowing the attacker to monitor and manipulate their data traffic.
4. Packet Sniffing: Hackers can use packet sniffing tools to capture and analyze the data packets traveling between devices and the public Wi-Fi network. This can reveal sensitive information transmitted in plaintext, particularly on unencrypted websites
5. Malware Distribution: Cybercriminals might inject malware into the data traffic of a public Wi-Fi network. When users connect, their devices could become infected with malicious software, leading to unauthorized access and data theft.
6. Session Hijacking: Attackers on the same network can hijack user sessions by stealing session cookies or tokens, which grant access to online accounts without needing login credentials.
7. Password Harvesting: Hackers can create fake login pages that mimic legitimate websites (a technique called phishing). When users enter their credentials, the hackers capture them for unauthorized access.
8. Exploiting Vulnerabilities: Public Wi-Fi networks can be targeted by attackers looking to exploit vulnerabilities in network hardware or software. These vulnerabilities might allow hackers to gain unauthorized access to the network itself.

Conclusion

In conclusion, public Wi-Fi networks offer convenience but also come with significant security risks. While they provide easy access to the internet in various locations, they lack the encryption and security measures found in private networks. Hackers can exploit these vulnerabilities to intercept data, steal sensitive information, and compromise devices.

Scenario 4 :Using Trial Version of Software

What is Software

Software refers to a collection of instructions, programs, data, and documentation that performs specific tasks on a computer or other digital devices. It is the intangible part of a computer system that enables it to carry out various functions and operations.

What is Trial version of software

A trial version of software is a limited or time-limited version of an application that software developers offer to users at no cost or a reduced price. These trial versions are designed to let users experience the software's functionalities before committing to purchasing the full version. They often provide access to core features, but certain advanced or premium functions might be disabled or restricted. Additionally, trial versions might include watermarks or branding on output files and come with a specific time limit, after which users are prompted to buy the full software. While trial versions are a way for developers to market their products, users should ensure they download such versions from official sources to avoid potential security risks.

Characteristics of trial versions of software are

1. **Limited Functionality:** Trial versions typically include most of the core features of the full software but may have certain features disabled, limited, or locked. This encourages users to experience the software's capabilities while leaving some of the more advanced or premium features for the full version.
2. **Time Limitation:** Many trial versions have a time limit during which they can be used. This could be a specific number of days (e.g., a 7-day trial) or a specific number of uses. After the trial period expires, users are often prompted to purchase the full version if they want to continue using the software.
3. **Watermarks or Branding:** Some trial versions include watermarks, logos, or other forms of branding on output files (such as images or documents) to discourage their use in professional settings without upgrading to the full version.
4. **No Technical Support:** Trial versions might not come with technical support, as this service is usually reserved for users who have purchased the full version.
5. **Upgrade Path:** Software developers offer trial versions as a way to entice users to purchase the full version. Usually, there is an easy transition from the trial version to the full version, either by purchasing a license key or subscribing to the software.
6. **Marketing Strategy:** Offering trial versions is a common marketing strategy for software companies. It allows potential customers to experience the software's benefits firsthand and helps them make an informed decision about whether the software meets their needs.

Benefits of using Trial versions of the Software.

Using trial versions of software offers several benefits to both users and software developers:

1. **Test Before Buying:** Trial versions allow users to test the software's features, functionalities, and user interface before committing to purchasing the full version. This helps users make informed decisions about whether the software meets their needs.
2. **Evaluate Compatibility:** Users can ensure that the software is compatible with their system configuration, hardware, and other software applications before investing in the full version.
3. **Explore Features:** Trial versions let users explore the core features of the software and get a feel for its capabilities. This exploration can help users understand how the software can enhance their workflow or productivity.
4. **Reduced Risk:** Trying a software's trial version before buying reduces the risk of purchasing software that doesn't meet expectations. Users can avoid spending money on software that might not be suitable for their needs.
5. **No Financial Commitment:** Since trial versions are often available for free or at a reduced cost, users can experiment with the software without a financial commitment. This is particularly helpful for individuals or businesses on a budget.
6. **Compare Alternatives:** Users can try out multiple software options within a specific category and compare their features, ease of use, and overall performance to make an informed choice.
7. **Early Learning:** Trial versions allow users to start learning the software's basics before making a purchase. This can lead to a smoother transition when moving to the full version.
8. **Potential Discounts:** Some software developers offer discounts or special offers to users who try the trial version. This can provide additional incentives for users to upgrade to the full version.

Conclusion

In conclusion, trial versions of software offer a valuable and convenient way for users to explore the functionalities and benefits of software applications without the immediate financial commitment. By allowing users to test software features, evaluate compatibility, and assess the overall suitability of the product, trial versions empower individuals and businesses to make well-informed decisions about software purchases. These trial versions also play a pivotal role in marketing strategies, enabling developers to showcase their software to a wider audience and gather user feedback for further improvement. With benefits such as reduced risk, the opportunity to learn and compare alternatives, and the potential for special offers, trial versions serve as a win-win solution for both users seeking the right software fit and developers striving to provide quality products and attract loyal customers.