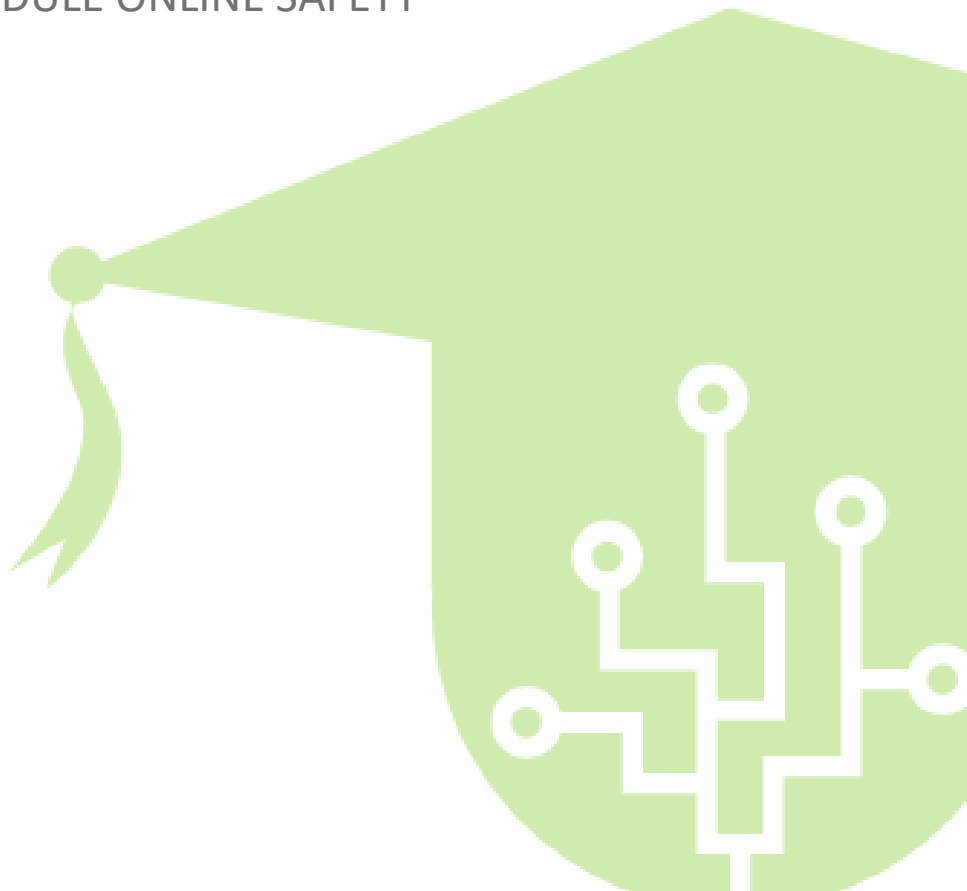


L2D

MEDIA LITERACY COMPETENCES
FOR YOUTH WORKERS

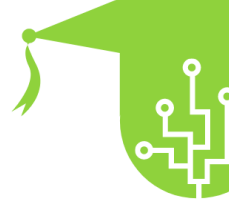
· GUIDELINES FOR SAFE ONLINE USE

MODULE ONLINE SAFETY

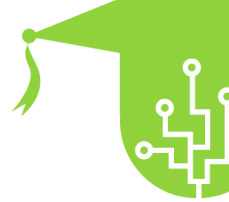




Title :	GUIDELINES FOR SAFE ONLINE USE
Key words :	Online Safety, Internet Security, Digital Privacy, Cybersecurity, Safe Online Practices, Personal Information Protection, Data Security, Password Management, Online Threats, Reporting Abuse, Privacy Settings
Prepared by .	
Language :	English
Objectives :	<ul style="list-style-type: none"> ● Define online safety: Explain the concept of online safety and its importance in today's digital world. ● Identify online threats: Help learners recognize various online threats such as phishing, malware, identity theft, cyberbullying, and scams. ● Understand privacy concerns: Educate participants about the significance of protecting personal information online and the potential consequences of privacy breaches. ● Develop strong passwords: Teach techniques for creating strong and unique passwords to enhance account security. ● Safeguard against phishing attempts: Provide strategies to detect and avoid falling victim to phishing emails, messages, and websites. ● Secure social media profiles: Offer guidelines for adjusting privacy settings, controlling the sharing of personal information, and handling friend requests. ● Promote safe online communication: Teach effective ways to communicate safely on social media, forums, and messaging platforms, emphasizing the avoidance of sharing sensitive details. ● Develop critical thinking skills: Foster the ability to evaluate information and sources critically, particularly in the context of fake news and misinformation online. ● Deal with online harassment and stalking: Offer guidance on how to respond to and report instances of online harassment or stalking.
Learning Outcomes :	
Content Index :	<ol style="list-style-type: none"> 1. INTERNET SAFETY <ol style="list-style-type: none"> 1.1.DEFINITION OF INTERNET SAFETY 1.2.UNDERSTANDING THE SCOPE AND IMPORTANCE <ol style="list-style-type: none"> 1.2.1. Scope of Internet Safety 1.2.2. Importance of Internet Safety



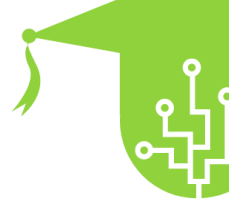
	<ul style="list-style-type: none"> 1.3.EVOLUTION OF INTERNET SAFETY CONCEPTS 1.4.Key Components of a Safe Online Experience 2. ONLINE THREATS <ul style="list-style-type: none"> 2.1.TYPES OF ONLINE THREATS 2.2.RECOGNIZING WARNING SIGNS 2.3.CONSEQUENCES OF IGNORING ONLINE THREATS 3. SAFEGUARDING PERSONAL INFORMATION <ul style="list-style-type: none"> 3.1. IMPORTANCE OF PRIVACY PROTECTION 3.2.SECURE ONLINE ACCOUNT MANAGEMENT 3.3.RESPONSIBLE SOCIAL MEDIA SHARING 4. NAVIGATING SOCIAL MEDIA SAFELY <ul style="list-style-type: none"> 4.1.ADJUSTING PRIVACY SETTINGS 4.2.HANDLING FRIEND REQUESTS AND MESSAGES 4.3.REPORTING AND BLOCKING ABUSIVE ACCOUNTS 5. CYBERSECURITY AND MOBILE DEVICES <ul style="list-style-type: none"> 5.1.SECURING SMARTPHONES AND TABLETS 5.2.APP PERMISSIONS AND DATA ACCESS 5.3.PROTECTING MOBILE DEVICES FROM THEFT AND LOSS
<p>Content Development :</p>	<ul style="list-style-type: none"> 1. INTERNET SAFETY <ul style="list-style-type: none"> 1.1. DEFINITION OF INTERNET SAFETY <p>Internet safety, also known as online safety, is the practice of adhering to actionable guidelines, gaining a comprehensive understanding of modern technology, and proactively safeguarding your digital devices to defend against the various malicious aspects of the online world.</p>



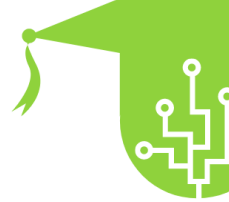
	<p>As the number of internet users continues to surge globally, various stakeholders, including governments, organisations, and internet service providers, have become increasingly concerned about the safety of vulnerable populations, such as children, teenagers, and the elderly, while they engage with the vast virtual realm. Alarming statistics reveal that over 45% of internet users have reported experiencing some form of cyber-harassment, underlining the urgent need for promoting safer online practices and cultivating a culture of digital responsibility.</p> <p>To address these pressing concerns and advocate for a safer digital landscape, Safer Internet Day is celebrated on a global scale every February. This annual event serves as a dedicated platform to raise awareness about internet safety, encouraging individuals and communities to be vigilant, informed, and proactive in their online interactions. Governments, non-profit organizations, and technology companies worldwide actively participate in Safer Internet Day initiatives, organizing awareness campaigns, educational workshops, and interactive events to equip internet users with the knowledge and skills necessary to navigate the online world securely.</p> <p>In the United Kingdom, the Get Safe Online campaign has emerged as a prominent force in promoting internet safety. With vital sponsorship from government agency Serious Organized Crime Agency (SOCA) and collaboration with major internet companies such as Microsoft and eBay, the campaign aims to empower internet users with practical guidance and resources to protect themselves against cyber threats. Through easily accessible information, tips, and tools, Get Safe Online strives to enhance the digital resilience of individuals, making the UK's internet community more robust and less susceptible to online dangers.</p> <p>As the internet continues to evolve and play an increasingly integral role in our daily lives, ensuring internet safety becomes paramount. By fostering a culture of responsible online behavior, raising awareness through initiatives like Safer Internet Day, and providing accessible resources like the Get</p>
--	---



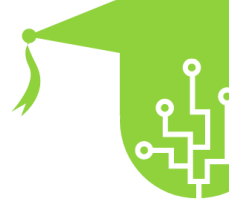
	<p>Safe Online campaign, we can collectively work towards creating a safer and more secure digital environment for everyone.</p> <p>In our ever-connected world, the importance of internet safety cannot be overstated. The internet offers unparalleled opportunities for learning, communication, and entertainment, but it also exposes users to potential risks and dangers. As technology advances and online threats become more sophisticated, staying informed and proactive about internet safety is crucial for individuals of all ages.</p> <p>For children and teenagers, who are often digital natives, understanding internet safety is essential for responsible and secure online interactions. Parents, educators, and guardians play a vital role in guiding young internet users, teaching them about the potential risks of sharing personal information, engaging with strangers, and participating in unsafe online activities.</p> <p>To enhance internet safety, it is crucial to stay updated on the latest cybersecurity trends and best practices. Regularly updating software and applications, using reputable antivirus software, and enabling automatic updates can fortify the defense of digital devices against emerging threats. Additionally, incorporating multi-factor authentication wherever possible adds an extra layer of protection to online accounts.</p> <p>Promoting a positive and safe online community also requires fostering digital empathy and respect. Encouraging kindness and empathy in online interactions can counter cyberbullying and toxic behavior, making the internet a more welcoming space for all.</p> <p>1.2. UNDERSTANDING THE SCOPE AND IMPORTANCE</p> <p>1.2.1. Scope of Internet Safety</p>
--	---



	<ul style="list-style-type: none"> ● Protection from cyber threats such as viruses, malware, phishing, ransomware, and identity theft. ● Safeguarding personal information and digital identity from unauthorized access and misuse. ● Navigating social media responsibly and dealing with cyberbullying or online harassment. ● Ensuring secure online transactions and protecting financial information while shopping or banking online. ● Safely using and managing mobile devices to avoid data breaches and privacy violations. ● Recognizing and avoiding online scams, fraudulent websites, and phishing attempts. ● Teaching children and teenagers about online safety and helping them develop responsible digital habits. <p style="text-align: center;">1.2.2. Importance of Internet Safety</p> <ul style="list-style-type: none"> ● Protection of Personal and Financial Information: Internet safety measures safeguard sensitive data, preventing identity theft and financial fraud. ● Maintaining Privacy and Digital Reputation: Being mindful of online activities helps individuals preserve their privacy and protect their digital reputation. ● Safeguarding Against Cyber Threats: Awareness of online risks and following security practices defend against cyber threats that can disrupt daily life, business operations, or compromise sensitive information. ● Empowering Positive Digital Experiences: Internet safety enables individuals to have positive, enriching experiences online without fear of harassment or victimization. ● Fostering Digital Citizenship: By practicing internet safety, individuals contribute to building a responsible and respectful digital community. ● Economic Impact: Cybersecurity incidents can have severe economic consequences for individuals, businesses, and governments, making internet safety an essential aspect of overall security.
--	--



	<ul style="list-style-type: none"> ● Protecting the Vulnerable: Internet safety is especially crucial for children, teenagers, and vulnerable populations who may be more susceptible to online dangers. <p style="text-align: center;">1.3. EVOLUTION OF INTERNET SAFETY CONCEPTS</p> <p>The "Evolution of Internet Safety Concepts" refers to how the understanding of internet safety and the measures taken to protect users from online threats have evolved over time. As the internet has grown and transformed, so have the challenges posed by cyber threats, leading to the development of new concepts and strategies to ensure online safety. This section delves into the historical context and the key milestones that have shaped internet safety practices.</p> <ul style="list-style-type: none"> ● Early Internet: In the early days of the internet, the concept of online safety was relatively simplistic. Most users were tech-savvy individuals or professionals who understood the risks associated with sharing personal information online. However, there was limited awareness among the general public about potential cyber threats. ● Rise of Online Communication: As online communication platforms and social media emerged, internet safety took on new dimensions. Users started sharing more personal information, leading to increased concerns about privacy and identity theft. Concepts like phishing and spam emails began to gain prominence as cybercriminals sought to exploit users' trust. ● Pioneering Cybersecurity Measures: With the growing threat landscape, cybersecurity measures began to evolve. Antivirus software, firewalls, and encryption technologies became essential tools for protecting against malware and unauthorized access. These early cybersecurity
--	---



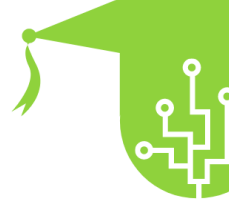
	<p>solutions laid the foundation for more advanced protection mechanisms in the future.</p> <ul style="list-style-type: none"> ● Awareness Campaigns and Initiatives: As cyber threats became more widespread, various organizations, governments, and tech companies started launching awareness campaigns and initiatives to educate the public about internet safety. These efforts aimed to raise awareness about common online risks and encourage users to adopt safer online practices. ● Growing Concerns about Cyberbullying: The rise of social media and online communication also brought attention to the issue of cyberbullying. As incidents of online harassment and cyberbullying increased, internet safety efforts expanded to address this form of digital aggression and support affected individuals. ● Mobile Internet and New Challenges: The advent of smartphones and mobile internet access introduced a new set of challenges for internet safety. The unique risks associated with mobile devices, such as app permissions and mobile malware, required tailored security measures. ● Advancements in Authentication: As passwords alone proved insufficient in protecting online accounts, two-factor authentication (2FA) and multi-factor authentication (MFA) gained popularity. These methods provided an additional layer of security, reducing the risk of unauthorized access. ● Emphasis on Digital Literacy: Internet safety concepts began to encompass not only technical security measures but also digital literacy and critical thinking skills. Educating users on identifying misinformation, fake news, and online scams became vital in combating online threats.
--	--



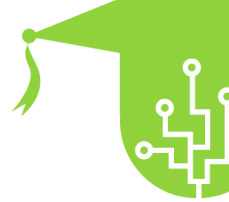
	<ul style="list-style-type: none"> ● The Rise of Cybersecurity Industry: The increasing sophistication of cyber threats gave rise to a robust cybersecurity industry. Companies and professionals specializing in cybersecurity services, threat analysis, and incident response played a crucial role in defending against evolving online risks. ● Integration of Internet Safety in Education: Recognising the importance of internet safety education, schools and educational institutions started incorporating it into their curriculum. Teaching children and young adults about responsible online behavior and digital citizenship became an essential aspect of modern education. <p>Media literacy is a teaching subject that was born with the aim of providing people with all the necessary tools to better understand the dynamics and messages offered by the media, and to rework them in an independent and critical way. Today, it's necessary to teach people to better manage their relationship with social media, to educate and train them on "what and how to post" or how to recognise "fake news". The use of the Internet thanks to smartphones offers infinite potential for learning, but also risks linked to the "superficial use of these tools". "Digital Immigrants" are most at risk because they are not used to dealing with the unwritten rules of a virtual world they do not belong to. They often don't know the main communication systems and don't have the ability to process new messages in order to offer their own contribution to the community, remaining passive elements.</p> <p>1.4. Key Components of a Safe Online Experience</p> <p>The "Key Components of a Safe Online Experience" are essential elements that contribute to creating a secure and protected environment while using the internet. These components encompass various practices, behaviors, and tools that individuals can</p>
--	---



	<p>employ to ensure their safety and privacy online. Understanding and implementing these key components are vital for a positive and secure internet experience.</p> <ul style="list-style-type: none"> ● Cybersecurity Awareness: Developing a strong cybersecurity awareness is fundamental to a safe online experience. This involves staying informed about the latest cyber threats, understanding common attack methods like phishing and malware, and recognizing warning signs of suspicious activities. Awareness empowers individuals to make informed decisions and take necessary precautions while navigating the digital world. ● Privacy Protection: Protecting one's privacy is a crucial aspect of internet safety. It involves being mindful of the information shared online and avoiding oversharing personal details. Safeguarding sensitive data, such as financial information and identification documents, is essential to prevent identity theft and fraud. ● Strong Authentication: Using robust authentication methods for online accounts is vital. This includes employing strong, unique passwords for each account and leveraging additional security layers like two-factor authentication (2FA) or biometric authentication when available. Strong authentication measures help prevent unauthorized access to accounts and protect sensitive information. ● Safe Browsing Practices: Practicing safe browsing habits is necessary to avoid malicious websites and potential threats. This includes verifying website URLs before entering sensitive information, avoiding clicking on suspicious links or pop-ups, and using secure browsers with built-in protections.
--	---



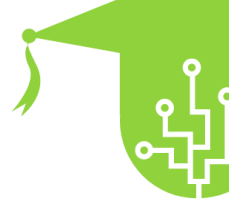
	<ul style="list-style-type: none"> ● Regular Software Updates: Keeping software, operating systems, and applications up to date is essential for maintaining a secure online experience. Regular updates often include security patches that address known vulnerabilities, making it harder for cybercriminals to exploit them. ● Secure Networks: Connecting to secure and trusted networks is critical for protecting data in transit. Avoiding public Wi-Fi networks without proper security measures is essential to prevent potential data interception and unauthorized access. ● Safe Social Media Practices: Being cautious while using social media platforms is crucial to protect personal information and avoid falling victim to social engineering attacks. Adjusting privacy settings, being selective about friend requests, and refraining from sharing sensitive data publicly are essential social media safety practices. ● Vigilance Against Phishing: Being vigilant against phishing attempts is vital. This involves verifying email senders' identities, not clicking on suspicious links or downloading attachments from unknown sources, and reporting phishing attempts. ● Parental Controls and Supervision: For parents and guardians, implementing parental controls and monitoring children's online activities are critical components of a safe internet experience for young users. This ensures age-appropriate content access and safeguards children from potentially harmful online content. ● Digital Literacy and Critical Thinking: Developing digital literacy and critical thinking skills is fundamental for identifying misinformation, fake news, and scams online.
--	---



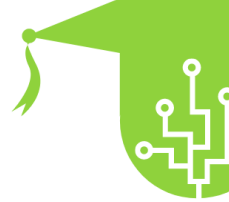
	<p>Understanding how to evaluate information sources and verify the credibility of content contributes to a safer online experience.</p> <p>2. ONLINE THREATS</p> <p>2.1. TYPES OF ONLINE THREATS</p> <p>Types of online threats refer to the various malicious activities and attacks that can jeopardize the security, privacy, and integrity of internet users and their data. Understanding these threats is crucial for individuals to take appropriate precautions and protect themselves while navigating the digital landscape. Here are some common types of online threats:</p> <p>Phishing: Phishing is a deceptive technique used by cybercriminals to trick users into revealing sensitive information, such as login credentials, financial details, or personal data. Phishing attempts often involve fake emails, websites, or messages that mimic legitimate entities to lure victims into providing their information.</p> <p>Malware: Malware is malicious software designed to infect and harm devices or networks. This includes viruses, worms, Trojans, ransomware, and spyware. Malware can compromise data, steal information, disrupt operations, or even render devices unusable.</p> <p>Ransomware: Ransomware is a specific type of malware that encrypts a user's data, effectively locking them out of their own files or systems. Cybercriminals demand a ransom payment to provide the decryption key, but there's no guarantee that paying the ransom will result in the return of the data.</p> <p>Social Engineering: Social engineering involves manipulating individuals to gain unauthorized access to sensitive information or systems. This can be done through impersonation, manipulation, or exploiting human psychology to deceive users into revealing confidential information.</p> <p>Data Breaches: A data breach occurs when cyber attackers gain unauthorized access to an organization's or individual's data. This may include personal information,</p>
--	--



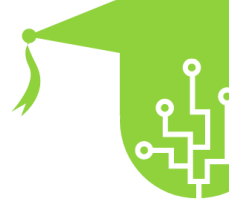
	<p>financial records, or intellectual property. Data breaches can have severe consequences for individuals' privacy and lead to identity theft or financial loss.</p> <p>Identity Theft: Identity theft involves stealing personal information, such as social security numbers, credit card details, or login credentials, to impersonate someone else for fraudulent purposes. Cybercriminals may use this stolen information for financial gain or to commit other crimes.</p> <p>Cyberbullying: Cyberbullying is a form of online harassment or bullying, typically occurring on social media platforms or through messaging apps. It involves sending hurtful messages, spreading rumors, or sharing embarrassing content with the intent to harm, intimidate, or humiliate the victim.</p> <p>Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: DoS and DDoS attacks aim to overwhelm a website or online service with a flood of traffic, rendering it inaccessible to legitimate users. These attacks can disrupt online services and cause financial losses for businesses.</p> <p>Man-in-the-Middle (MitM) Attacks: MitM attacks involve intercepting and eavesdropping on communication between two parties, such as a user and a website. The attacker can then view or manipulate the data exchanged without the knowledge of the communicating parties.</p> <p>Zero-Day Exploits: Zero-day exploits target software vulnerabilities that are not yet known to the vendor or developers. Cybercriminals use these vulnerabilities to launch attacks before a patch or fix is available, making them challenging to defend against.</p> <p>Internet of Things (IoT) Vulnerabilities: As more devices become connected to the internet, IoT vulnerabilities have become a concern. Weak security measures in IoT devices can be exploited to gain access to home networks or compromise privacy.</p> <p>2.2. RECOGNISING WARNING SIGNS</p> <p>Recognizing warning signs is a crucial skill when it comes to internet safety. It involves being alert to indicators that</p>
--	---



	<p>something may be amiss or potentially harmful while using the internet. By recognizing warning signs, individuals can take prompt action to protect themselves from online threats and avoid falling victim to scams, cyberattacks, or other malicious activities. Here are some key warning signs to watch for:</p> <p>Unsolicited Communication: Be cautious of unsolicited emails, messages, or friend requests from unknown or suspicious sources. Cybercriminals often use these means to initiate phishing attempts or deliver malware.</p> <p>Poor Grammar and Spelling: Many phishing emails and scam messages contain grammatical errors, misspellings, or awkward language. These mistakes can be a sign that the communication is not from a legitimate source.</p> <p>Requests for Personal Information: Be wary of requests for sensitive information, such as login credentials, financial details, or social security numbers, especially if the request comes unexpectedly or seems unnecessary.</p> <p>Urgent or Threatening Language: Messages that use urgent or threatening language to pressure you into taking immediate action could be indicators of a scam or phishing attempt.</p> <p>Unusual Links or URLs: Hover your mouse over links in emails or messages to see the actual URL destination. Be cautious of shortened URLs or links that redirect to suspicious websites.</p> <p>Mismatched or Fake URLs: Be mindful of URLs that appear to be legitimate but have subtle misspellings or variations. Scammers may use domain names that closely resemble well-known websites to deceive users.</p> <p>Unfamiliar Email Senders: Verify the identity of email senders, especially if the message contains unexpected attachments or requests for sensitive information.</p> <p>Unexpected Downloads: Be cautious of any downloads or attachments that you didn't initiate or weren't expecting, as they may contain malware.</p> <p>Unusual Account Activity: Regularly review your online account activity and be alert to any unauthorized logins or transactions.</p>
--	---



	<p>Unexplained System Behavior: If your computer or device is behaving unusually, such as frequent crashes, slowdowns, or unexpected pop-ups, it could indicate malware or other security issues.</p> <p>Warnings from Security Software: Pay attention to warnings or alerts from your antivirus or security software, as they may indicate potential threats or suspicious activities.</p> <p>Unsolicited Offers and Promotions: Be cautious of unsolicited offers or promotions that seem too good to be true, as they may be scams attempting to lure you into providing personal information.</p> <p style="text-align: center;">2.3. CONSEQUENCES OF IGNORING ONLINE THREATS</p> <p>Ignoring online threats can have serious and far-reaching consequences that can negatively impact individuals, businesses, and even society as a whole. Failing to address or take appropriate action against online threats can leave one vulnerable to various cyber risks, leading to financial loss, privacy breaches, reputational damage, and even legal repercussions. Here are some key consequences of ignoring online threats:</p> <p>Financial Loss: Falling victim to scams, phishing attacks, or fraudulent online schemes can result in significant financial losses. Cybercriminals may steal banking credentials, credit card information, or conduct unauthorized transactions, leading to drained bank accounts and financial hardships.</p> <p>Identity Theft: Ignoring warning signs of identity theft can allow cybercriminals to steal personal information, such as social security numbers, birthdates, and addresses. They can use this stolen information to commit financial fraud, open accounts in the victim's name, or engage in other criminal activities, causing severe long-term consequences for the victim.</p> <p>Data Breaches: Failing to implement robust security measures or address vulnerabilities can lead to data breaches for individuals and organizations. A data breach can expose sensitive information, including customer data, trade secrets, or intellectual property, resulting in financial penalties, legal liabilities, and damage to the organization's reputation.</p>
--	---



	<p>Ransomware Attacks: Ignoring cybersecurity practices can make individuals and businesses susceptible to ransomware attacks. When systems are compromised by ransomware, valuable data can be encrypted, and attackers demand payment for the decryption key. Paying the ransom doesn't guarantee data recovery, and victims may suffer data loss or operational disruptions.</p> <p>Reputational Damage: Falling prey to cyberbullying or social media attacks can cause significant reputational damage to individuals and organisations. False information, negative reviews, or harmful content spread online can harm personal or brand reputation, affecting social standing, professional opportunities, and customer trust.</p> <p>Loss of Privacy: Ignoring privacy concerns can lead to the exposure of private information, including personal conversations, images, or videos. This loss of privacy can have emotional and psychological consequences, as well as potential blackmail threats.</p> <p>Legal Consequences: Ignorance of cyber threats and failing to implement necessary security measures may lead to legal consequences. Individuals or organizations may face legal actions, fines, or regulatory penalties for data breaches, privacy violations, or non-compliance with cybersecurity standards.</p> <p>Disruption of Services: Businesses that ignore online threats may experience disruptions to their operations. Cyberattacks, such as distributed denial of service (DDoS) attacks, can overload websites or networks, rendering services inaccessible to customers and resulting in loss of revenue and credibility.</p> <p>Social and Emotional Impact: Ignoring cyberbullying, online harassment, or predatory behavior can have severe social and emotional consequences for victims. It can lead to anxiety, depression, self-isolation, and even thoughts of self-harm.</p> <p>National Security Concerns: Ignoring online threats can extend beyond individual or organisational levels and become a matter of national security. Cyberattacks on critical infrastructure or government systems can disrupt essential services, compromise sensitive information, and undermine national stability.</p> <p>3. SAFEGUARDING PERSONAL INFORMATION</p>
--	--



3.1. IMPORTANCE OF PRIVACY PROTECTION

Privacy protection is of paramount importance in today's digital age due to the widespread use of technology and the internet. It refers to safeguarding an individual's personal information, data, and online activities from unauthorized access, misuse, and exploitation. The significance of privacy protection can be understood from various perspectives:

Personal Security and Safety: Protecting privacy ensures that sensitive personal information, such as social security numbers, financial data, or home addresses, remains confidential and secure. Preventing unauthorized access to this information helps prevent identity theft, financial fraud, and other forms of cybercrimes that can have severe consequences for individuals.

Data Privacy and Control: Individuals have the right to control how their data is collected, stored, and used by organizations. Privacy protection ensures that individuals can make informed choices about sharing their data and consent to its use for specific purposes.

Maintaining Trust: Privacy protection is essential for building and maintaining trust between individuals and organizations. When users trust that their personal information will be handled responsibly and securely, they are more likely to engage with online services, conduct transactions, and share information with confidence.

Preserving Personal Freedom: Respecting privacy means allowing individuals to express themselves freely, without fear of surveillance or discrimination based on their online activities or preferences. Privacy protection is essential to uphold the right to freedom of speech and expression.

Preventing Online Harassment and Stalking: Privacy protection safeguards individuals from online harassment and stalking. By restricting access to personal information, privacy measures reduce the risk of targeted attacks or cyberbullying.

Protecting Personal Relationships: Privacy protection allows individuals to communicate and share information within the confines of trusted relationships, ensuring that private conversations and interactions remain confidential.



Avoiding Data Misuse: Privacy protection mitigates the risk of personal data being exploited for purposes other than those intended by the individual. This includes avoiding unwanted marketing campaigns, spam emails, or personalized content that could infringe on personal space.

Preventing Discrimination and Profiling: Protecting privacy can help prevent the profiling and discrimination of individuals based on their personal information or online behavior. Data collection without adequate privacy protections can lead to unfair and biased decision-making.

Cybersecurity and Digital Trust: Privacy protection and cybersecurity are interconnected. A breach of privacy can lead to cybersecurity incidents and vice versa. By prioritizing privacy, individuals and organizations can foster a culture of digital trust and security.

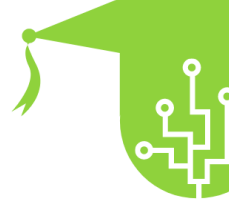
3.2. SECURE ONLINE ACCOUNT MANAGEMENT

Secure online account management is a set of practices and strategies aimed at protecting and managing one's online accounts in a way that minimizes the risk of unauthorized access and data breaches. Proper online account management is crucial for maintaining the privacy of personal information, preventing identity theft, and safeguarding digital assets. Here are some key aspects and best practices for secure online account management:

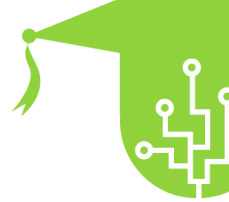
Strong and Unique Passwords: Use strong and unique passwords for each online account. Avoid using easily guessable passwords, such as "123456" or "password." Instead, create complex passwords with a mix of uppercase and lowercase letters, numbers, and special characters.

Password Managers: Consider using a reputable password manager to generate, store, and manage passwords securely. Password managers help you maintain strong and unique passwords for each account without the need to remember them all.

Enable Two-Factor Authentication (2FA): Whenever possible, enable two-factor authentication for your online accounts. 2FA adds an extra layer of security by requiring a second form of verification, such as a one-time code sent to your mobile device, in addition to your password.



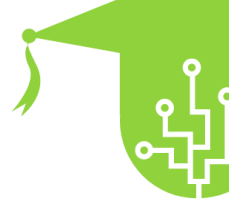
	<p>Monitor Account Activity: Regularly review your account activity and be vigilant for any unauthorized logins or suspicious actions. If you notice any unusual activity, take immediate action to secure your account, such as changing your password and contacting the account provider.</p> <p>Avoid Public Computers and Wi-Fi: Refrain from accessing sensitive accounts, such as email or banking, from public computers or unsecured Wi-Fi networks. Public computers may store login credentials, and unsecured Wi-Fi can expose your data to potential eavesdropping.</p> <p>Beware of Phishing Attempts: Be cautious of unsolicited emails, messages, or links that request sensitive information or prompt you to log in to your accounts. Verify the legitimacy of the sender and website before providing any information.</p> <p>Regularly Update Account Recovery Information: Keep your account recovery information, such as alternate email addresses or phone numbers, up to date. This ensures that you can regain access to your account if you forget your password or encounter other login issues.</p> <p>Review Privacy and Security Settings: Periodically review the privacy and security settings of your online accounts. Adjust the settings according to your preferences and needs to ensure the right balance between privacy and functionality.</p> <p>Log Out and Secure Devices: Always log out of your accounts when you finish using them, especially on shared or public devices. Additionally, secure your personal devices with strong passwords or biometric authentication.</p> <p>Regularly Change Passwords: Consider changing your passwords periodically, especially for critical accounts like email and banking. Regularly updating passwords adds an extra layer of security.</p> <p>Enable Account Recovery Options: Set up account recovery options, such as security questions or backup codes, to regain access to your account in case you are locked out.</p> <p style="text-align: center;">3.3. RESPONSIBLE SOCIAL MEDIA SHARING</p>
--	--



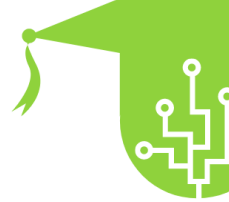
	<p>Responsible social media sharing refers to the conscious and mindful approach of sharing content on social media platforms in a way that respects privacy, promotes positive interactions, and avoids contributing to misinformation or harm. Practicing responsible social media sharing is crucial for maintaining digital etiquette, fostering a positive online community, and protecting both personal and collective well-being. Here are some key aspects of responsible social media sharing:</p> <p>Protecting Personal Information: Be cautious about sharing sensitive personal information, such as home addresses, phone numbers, or financial details, on social media. Protecting personal information helps safeguard against identity theft and other privacy-related risks.</p> <p>Adjusting Privacy Settings: Regularly review and adjust your privacy settings on social media platforms. Customize the audience for each post, ensuring that only the intended audience can view and interact with your content.</p> <p>Respecting Consent: Obtain consent from individuals before sharing their photos or personal information on social media. Be considerate of people's preferences regarding being tagged in posts or mentioned in content.</p> <p>Fact-Checking and Avoiding Misinformation: Before sharing news articles, information, or images, verify their accuracy from reliable sources. Avoid spreading misinformation or unverified content that may contribute to the spread of rumors or false narratives.</p> <p>Being Mindful of Timing and Frequency: Avoid excessive or inappropriate sharing, as it may lead to information overload for your followers. Be mindful of the timing of your posts to respect different time zones and the preferences of your audience.</p> <p>Promoting Positive Content: Share content that is uplifting, informative, or inspiring. Positive sharing contributes to a healthier online environment and fosters a sense of community among your followers.</p> <p>Handling Disagreements Respectfully: Engage in respectful and constructive discussions on social media, even when disagreeing with others. Avoid engaging in online arguments or resorting to personal attacks.</p>
--	--



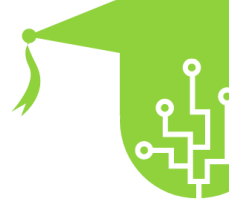
	<p>Avoiding Harmful or Offensive Content: Refrain from sharing content that may be offensive, discriminatory, or harmful to others. Be aware of the potential impact of your posts on different individuals and communities.</p> <p>Protecting Copyrights: Respect copyright laws and avoid sharing copyrighted material without proper authorization or attribution. Give credit to the original creators when sharing their work.</p> <p>Reviewing Shared Content: Regularly review your shared content to ensure it aligns with your values and the image you want to portray online. Delete or update posts that may no longer reflect your current perspectives.</p> <p>Promoting Digital Kindness: Be kind and empathetic in your interactions on social media. Avoid participating in or spreading cyberbullying, hate speech, or any form of harmful behavior.</p> <p>Encouraging a Positive Online Culture: Encourage others to practice responsible social media sharing by setting a positive example. Engage in discussions about digital citizenship and the importance of being responsible digital citizens.</p> <p>4. NAVIGATING SOCIAL MEDIA SAFELY</p> <p>4.1. ADJUSTING PRIVACY SETTINGS</p> <p>Adjusting privacy settings refers to the process of customizing the level of access and visibility of personal information on various platforms, websites, and applications. It involves making informed choices about what data is shared, with whom it is shared, and how it is used by third parties. By adjusting privacy settings, individuals can maintain greater control over their digital footprint and protect their personal information from unnecessary exposure. Here's a detailed explanation of the importance and steps involved in adjusting privacy settings:</p> <p>Importance of Adjusting Privacy Settings:</p> <p>Protecting Personal Information: Adjusting privacy settings allows individuals to limit the amount of personal information visible to others, reducing the risk of identity theft, stalking, or social engineering attacks.</p>
--	---



	<p>Controlling Data Sharing: By customizing privacy settings, individuals can control what data they share with social media platforms, websites, and apps, limiting the collection and usage of their information.</p> <p>Preventing Targeted Advertising: Privacy settings can help individuals opt-out of targeted advertising and personalized content, providing a more private and less intrusive online experience.</p> <p>Avoiding Data Misuse: Adjusting privacy settings reduces the chances of data misuse by unauthorized third parties, protecting against potential breaches and unauthorized access to sensitive information.</p> <p>Enhancing Online Security: Restricting access to personal information through privacy settings can enhance online security and minimize the risk of social engineering or phishing attacks.</p> <p>Steps for Adjusting Privacy Settings:</p> <p>Review Account Settings: On social media platforms, review the account settings or privacy settings section to access the options for customizing privacy preferences.</p> <p>Choose Audience for Posts: Determine who can view your posts, such as friends, friends of friends, or the public. Opt for a narrower audience to limit the visibility of your content.</p> <p>Control Profile Information: Decide what profile information is visible to others, such as your email address, phone number, or date of birth. Minimize the visibility of sensitive data if possible.</p> <p>Manage App Permissions: In mobile apps, review and manage app permissions in the device settings. Allow only the necessary permissions for each app and revoke permissions for apps that don't require them.</p> <p>Opt-Out of Data Collection: Some platforms and websites offer the option to opt-out of data collection and sharing for advertising purposes. Take advantage of these options to reduce data tracking.</p> <p>Customize Location Sharing: Choose when and with whom you share your location. Turn off location sharing when not needed or limit it to specific trusted apps.</p>
--	---



	<p>Consider Anonymous Browsing: Use private or incognito browsing modes to prevent the storage of browsing history and cookies on your device.</p> <p>Check Third-Party App Access: Review and manage third-party apps that have access to your account information. Revoke access for apps that are no longer in use or don't need access.</p> <p>Be Cautious of Default Settings: Many platforms have default privacy settings that may be more permissive than desired. Take the time to adjust these settings according to your preferences.</p> <p>Regularly Review and Update: Periodically review and update your privacy settings as platforms and apps may introduce new features or changes that affect your privacy.</p> <p style="text-align: center;">4.2. HANDLING FRIEND REQUESTS AND MESSAGES</p> <p>Handling friend requests and messages on social media platforms and messaging apps involves being cautious, discerning, and respectful in your interactions with others. It's essential to maintain personal boundaries, protect your privacy, and foster a positive online experience. Here are some guidelines for handling friend requests and messages:</p> <p>Handling Friend Requests:</p> <p>Verify Identity: Before accepting a friend request, ensure you know the person or have mutual friends. Be cautious about accepting requests from unfamiliar or suspicious profiles.</p> <p>Check Privacy Settings: Adjust your privacy settings to control who can send you friend requests. Limit friend requests to friends of friends or specific groups to reduce the chances of receiving requests from strangers.</p> <p>Avoid Accepting Strangers: Be selective about adding new connections. Avoid accepting friend requests from individuals you don't know personally, especially if they have no mutual connections.</p>
--	---



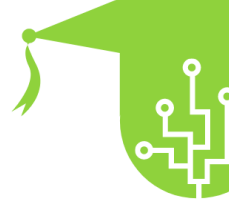
	<p>Block or Report Suspicious Accounts: If you receive friend requests from suspicious or fake accounts, consider blocking or reporting them to the platform administrators.</p> <p>Review Profile Information: Before accepting a friend request, review the requester's profile to ensure it appears genuine and aligns with your values and interests.</p> <p>Respect Boundaries: It's okay to decline friend requests if you are not comfortable connecting with someone. Respect your own boundaries and don't feel obligated to accept every request.</p> <p>Handling Messages:</p> <p>Be Respectful: Respond to messages in a polite and respectful manner. Treat others how you would like to be treated in an online conversation.</p> <p>Verify Senders: If you receive a message from an unfamiliar sender, exercise caution. Avoid clicking on suspicious links or downloading attachments from unknown sources.</p> <p>Avoid Sharing Sensitive Information: Refrain from sharing sensitive personal information, financial details, or passwords through messaging apps. Be cautious about sharing private information with individuals you don't know well.</p> <p>Report Harassment or Abuse: If you receive offensive, threatening, or harassing messages, report the sender to the platform administrators or the messaging app's support team.</p> <p>Set Message Privacy: Adjust your message privacy settings to control who can send you messages. Limit messaging access to your friends or contacts.</p> <p>Use Blocking Feature: If someone is bothering you or sending inappropriate messages, use the blocking feature to prevent further contact from that person.</p> <p>Be Mindful of Tone and Intent: Messages can be easily misinterpreted due to the lack of tone and facial expressions. Be mindful of your own communication and try to avoid misunderstandings.</p>
--	---



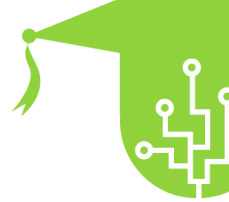
	<p>Take Breaks from Messaging: It's okay to take breaks from messaging and social media to focus on other activities and reduce digital overwhelm.</p> <p style="text-align: center;">4.3. REPORTING AND BLOCKING ABUSIVE ACCOUNTS</p> <p>Reporting and blocking abusive accounts is a crucial step in maintaining a safe and positive online environment. Abusive accounts can engage in harmful behavior, such as cyberbullying, harassment, hate speech, and other forms of online abuse. Reporting and blocking these accounts help protect yourself and others from their harmful actions. Here's an explanation of how reporting and blocking work and why they are important:</p> <p>Reporting Abusive Accounts:</p> <p>Identify Harmful Behavior: If you come across an account that is engaging in abusive or harmful behavior, such as harassment, threats, or hate speech, it's important to recognize it.</p> <p>Report the Account: Most social media platforms and online services have a reporting mechanism. Use the platform's reporting feature to inform the administrators or moderators about the abusive behavior.</p> <p>Provide Evidence: When reporting an abusive account, it can be helpful to provide evidence, such as screenshots or links to the offensive content, to support your report.</p> <p>Choose the Appropriate Category: Social media platforms often offer different reporting categories. Select the category that best fits the type of abuse you are reporting.</p> <p>Respect Reporting Guidelines: Familiarize yourself with the platform's reporting guidelines to ensure that you're reporting accounts for valid reasons. Avoid false reporting, as it can hinder the effectiveness of the reporting system.</p> <p>Blocking Abusive Accounts:</p> <p>Protect Yourself: Blocking an abusive account prevents that account from interacting with you. It can help protect your mental well-being and create a safe online space for you.</p>
--	--



	<p>Prevent Unwanted Contact: When you block an account, the user behind that account won't be able to follow you, send you messages, or comment on your posts.</p> <p>Anonymity: Blocking is usually a private action. The user you block will not receive any notification that they have been blocked.</p> <p>No Further Interaction: After blocking an account, you will no longer see any of their content or activity, and they won't be able to see yours.</p> <p>Why Reporting and Blocking Are Important:</p> <p>Preventing Harm: Reporting abusive accounts can lead to action being taken against the account, which can prevent further harm to you or others.</p> <p>Enforcing Platform Guidelines: Reporting abusive behavior helps enforce the platform's terms of service and community guidelines, creating a safer environment for all users.</p> <p>Supporting Community Health: By reporting and blocking abusive accounts, you contribute to fostering a healthy and respectful online community.</p> <p>Empowering Users: Reporting and blocking empower individuals to take control of their online experiences and protect themselves from abusive or harmful interactions.</p> <p>5. CYBERSECURITY AND MOBILE DEVICES</p> <p>5.1. SECURING SMARTPHONES AND TABLETS</p> <p>Securing smartphones and tablets is essential in today's mobile-driven world, where these devices store a wealth of personal information and sensitive data. Securing these devices helps protect against unauthorized access, data breaches, and malware attacks. Here are some key measures to ensure the security of smartphones and tablets:</p> <p>Enable Lock Screen Security: Set up a secure lock screen method, such as a PIN, pattern, password, or biometric (fingerprint or face recognition). This prevents unauthorized access to your device if it is lost or stolen.</p>
--	---



	<p>Keep Software Up to Date: Regularly update the operating system and applications on your device. Manufacturers release updates to fix security vulnerabilities, so keeping your device updated is crucial to stay protected against potential exploits.</p> <p>Install Trusted Apps Only: Download apps from official app stores (e.g., Google Play Store, Apple App Store) and avoid installing apps from unknown sources. Malicious apps from unofficial sources can compromise your device's security and privacy.</p> <p>Review App Permissions: Be cautious when granting permissions to apps. Review the permissions requested by each app and consider whether they are necessary for the app's functionality. Avoid granting unnecessary permissions that may compromise your privacy.</p> <p>Use a VPN on Public Wi-Fi: When using public Wi-Fi networks, consider using a virtual private network (VPN) to encrypt your internet traffic and protect your data from potential eavesdropping or snooping.</p> <p>Secure Mobile Browsing: Use secure browsers that offer encrypted connections (HTTPS) for websites. Avoid accessing sensitive information, such as online banking, on unsecured or public networks.</p> <p>Backup Data Regularly: Back up your device's data regularly to a secure cloud service or an external device. This ensures that your important information is safe even if your device is lost, damaged, or reset.</p> <p>Avoid Clicking on Suspicious Links: Be cautious of clicking on links in emails, messages, or pop-ups from unknown sources. Clicking on malicious links can lead to phishing attempts or the installation of malware.</p> <p>Use App Locks for Sensitive Apps: Consider using app locks or a guest mode feature to restrict access to sensitive apps or content on your device. This provides an additional layer of security, especially when sharing your device with others.</p> <p>Encrypt Device Data: If your device supports it, enable encryption to protect your data from unauthorized access even if the device is physically accessed by someone else.</p>
--	--



5.2. APP PERMISSIONS AND DATA ACCESS

App permissions and data access refer to the permissions requested by mobile applications (apps) to access various features and data on a user's device. When users install and use apps on their smartphones or tablets, the apps may require access to certain device resources and personal information to function properly. These permissions enable apps to deliver specific functionalities and enhance user experience. However, it's essential for users to understand and manage these permissions to protect their privacy and security. Here's a closer look at app permissions and data access:

Types of App Permissions: App permissions can vary depending on the app's functionality and the platform (Android or iOS). Common types of app permissions include access to the device's camera, microphone, location, contacts, calendar, storage, SMS, call logs, and more. Some apps may also request permission to use other connected devices, such as Bluetooth peripherals.

Permission Requests: When users install an app, the app may request specific permissions that it needs to operate. Permission requests are usually presented during the app installation process or when the app first attempts to access a particular feature. Users can either grant or deny these permissions.

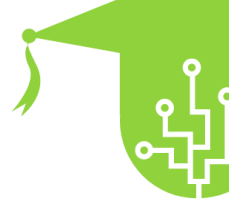
Purpose of App Permissions: App permissions are necessary to enable certain app features. For example, a photo-editing app needs access to the device's camera and storage to capture and save photos. A navigation app requires location access to provide accurate directions.

Protecting Privacy: While app permissions are often essential for app functionality, users should be cautious about granting permissions without considering the app's purpose and whether the requested permissions are reasonable. Granting excessive permissions could potentially compromise privacy or allow apps to access sensitive data without a legitimate need.

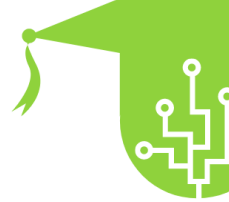
Managing App Permissions: Most modern operating systems allow users to manage app permissions. Users can review and modify app permissions in the device settings,



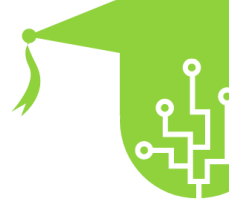
	<p>enabling them to grant or revoke specific permissions for individual apps at any time.</p> <p>Reading Permissions Carefully: Before granting permissions, users should carefully read the permissions requested by an app. If an app requests permissions that seem unrelated to its functionality, it may be a red flag, and users should exercise caution or consider using alternative apps.</p> <p>App Permissions and Updates: When updating apps, it's essential to review any new or changed permissions. Sometimes, app updates may introduce additional permissions, and users should ensure that they align with their preferences and needs.</p> <p>App Permission Requests for iOS and Android: While iOS and Android handle app permissions differently, both platforms offer users the ability to manage permissions in their respective settings. On iOS, users can review and manage permissions in the app settings under "Privacy." On Android, users can manage permissions by going to "Apps & notifications" or "Application manager" in device settings.</p> <p style="text-align: center;">5.3. PROTECTING MOBILE DEVICES FROM THEFT AND LOSS</p> <p>Protecting mobile devices from theft and loss is crucial to safeguard personal information, prevent identity theft, and preserve the privacy of sensitive data. Mobile devices, such as smartphones and tablets, are often targets for thieves due to their portability and the valuable information they store. Implementing security measures can significantly reduce the risks associated with theft or loss. Here are some important steps to protect mobile devices:</p> <p>Set Up Lock Screen Security: Enable a secure lock screen method, such as a PIN, pattern, password, or biometric (fingerprint or face recognition). This prevents unauthorized access to your device if it falls into the wrong hands.</p> <p>Use Find My Device Services: Enable the "Find My Device" or "Find My iPhone" feature on your device. These services allow you to locate, lock, or erase your device remotely if it gets lost or stolen.</p>
--	---



	<p>Keep Software and Apps Updated: Regularly update your device's operating system and apps to ensure you have the latest security patches and bug fixes. Manufacturers release updates to address vulnerabilities and improve device security.</p> <p>Avoid Leaving Devices Unattended: Be cautious about leaving your mobile device unattended in public places, such as restaurants, public transportation, or gyms. Keep your device with you or securely stored to reduce the risk of theft.</p> <p>Stay Vigilant in Crowded Areas: Pay attention to your surroundings in crowded areas, especially where pickpocketing and theft are more likely to occur. Be cautious when using your device in crowded spaces.</p> <p>Securely Store Your Device at Home: Keep your mobile device in a secure location when not in use, especially at home. Avoid leaving it on counters, near open windows, or easily accessible areas.</p> <p>Use App Locks for Sensitive Apps: Consider using app locks or guest mode features to restrict access to sensitive apps or content on your device. This adds an extra layer of security, especially when sharing your device with others.</p> <p>Encrypt Device Data: If your device supports it, enable encryption to protect your data from unauthorised access, even if the device is physically accessed by someone else.</p> <p>Avoid Public Charging Stations: Refrain from using public charging stations or USB ports, as they may be compromised and pose a risk of data theft or malware installation.</p> <p>Backup Data Regularly: Back up your device's data regularly to a secure cloud service or an external device. This ensures that your important information is safe even if your device is lost, damaged, or reset.</p> <p>Use Privacy Screen Protectors: Consider using privacy screen protectors to prevent prying eyes from viewing your screen in public spaces.</p> <p>Register Devices with Authorities: Register your mobile devices with local authorities or relevant databases. This can aid in the recovery process if your device is stolen.</p>
<p>Glossary :</p>	<p>1. Online Safety</p>



	<p>The practice of following actionable guidelines, understanding modern technology, and protecting digital devices to defend against malicious parts of the online world.</p> <p>2. Internet Security Measures and practices taken to protect computers, networks, and data from cyber threats, such as malware, viruses, and unauthorized access.</p> <p>3. Digital Privacy The right to control and protect one's personal information and data from being accessed, used, or shared without consent.</p> <p>4. Cybersecurity The protection of digital devices, networks, and information systems from cyber threats, including hacking, data breaches, and cyberattacks.</p> <p>5. Safe Online Practices The set of guidelines and behaviors that individuals should follow to ensure their online activities are secure and protect their privacy.</p> <p>6. Personal Information Protection The safeguarding of sensitive and personal data from unauthorized access or misuse, preventing identity theft and fraud.</p> <p>7. Social Media Etiquette The proper and respectful behavior that individuals should adhere to when using social media platforms.</p> <p>8. Data Security Measures and protocols taken to protect digital data from unauthorized access, modification, or destruction.</p> <p>9. Identity Theft Prevention Techniques and practices to safeguard personal information and prevent criminals from using it to impersonate individuals.</p> <p>10. Password Management The responsible practice of creating strong, unique passwords and managing them securely to protect online accounts.</p> <p>11. Online Threats</p>
--	--



	<p>Various risks and dangers encountered while using the internet, such as phishing, malware, scams, and cyberbullying.</p> <p>12. Phishing Awareness The ability to recognize and avoid phishing attempts, where attackers deceive individuals to obtain sensitive information, often through fraudulent emails or websites.</p> <p>13. Privacy Settings The customizable options on online platforms that allow users to control the visibility of their personal information and the audience for their content.</p> <p>14. Reporting Abuse The process of informing platform administrators or moderators about abusive or harmful behavior on the platform, such as harassment or hate speech.</p> <p>15. Blocking Accounts The action of preventing an abusive or unwanted account from interacting with you or viewing your content on social media platforms.</p> <p>16. Secure Online Transactions Ensuring that online transactions, such as purchases or financial transactions, are conducted safely and securely to prevent fraud.</p> <p>17. Digital Footprint The trail of data and information left behind by an individual's online activities, including social media posts, search history, and online interactions.</p> <p>18. Cyberbullying Prevention Measures taken to stop and prevent online harassment, intimidation, or bullying.</p> <p>19. Two-Factor Authentication (2FA) An additional layer of security that requires users to provide two forms of identification (e.g., password and a unique code sent to their phone) to access an account.</p> <p>20. Safe Browsing Habits Practices and guidelines to ensure secure and safe internet browsing, avoiding risky websites and content.</p>
<p>Bibliography :</p>	<p>Internet Safety Tips & Internet Safety Rules (kaspersky.com)</p>



	<p>Online Safety (for Teens) - Nemours KidsHealth</p> <p>What is Online Safety? SWGfL</p> <p>Online safety conversation LearnEnglish Teens (britishcouncil.org)</p> <p>Internet safety - Wikipedia</p> <p>Online safety issues - Advice to support children Internet Matters</p> <p>Internet Safety: Introduction to Internet Safety (gcfglobal.org)</p> <p>indianjournals.com/ijor.aspx?target=ijor:ijie&volume=8&issue=2&article=001</p> <p>"Internet Safety" in: The International Encyclopedia of Media Literacy Online (researchgate.net)</p> <p>İnternette Güvenlik İpuçları - Google Güvenlik Merkezi (safety.google)</p> <p>Being safe online eSafety Commissioner</p> <p>How to Stay Safe Online: Internet Safety Tips and Resources (reviews.org)</p>
<p>Resources (videos, reference link)</p>	<p>https://www.youtube.com/watch?v=qZE45J-MIUg&pp=ygULc2FmZSBvbmxpbmU%3D</p> <p>https://www.youtube.com/watch?v=aO858HyFbKI&pp=ygULc2FmZSBvbmxpbmU%3D</p> <p>https://www.youtube.com/watch?v=HxySrSbSY7o&pp=ygULc2FmZSBvbmxpbmU%3D</p> <p>https://www.youtube.com/watch?v=EyQeUwqCDWg&pp=ygULc2FmZSBvbmxpbmU%3D</p>