WHY INTERNET SECURITY MATTERS

1. **Identity Theft:** Hackers may steal your personal information, such as your name, address, and financial details, to commit fraud or access your accounts.
2. **Financial Loss:** Cybercriminals can use malware or phishing attacks to gain access to your bank accounts or credit card information, leading to financial loss.
3. **Privacy Breaches:** Without adequate security, your online activities and private information could be accessed by unauthorized parties, compromising your privacy.
4. **Data Breaches:** Businesses and organizations can suffer data breaches, resulting in the exposure of sensitive customer information, leading to reputation damage and legal consequences.
5. **Malware Infections:** Malicious software (malware) can infect your devices, causing damage, stealing data, or giving hackers control over your system.

HOW TO STAY SAFE ON THE INTERNET

1. **Use Strong Passwords:** Create unique and complex passwords for your online accounts. Avoid using easily guessable passwords and consider using a password manager to securely store and manage your passwords.
2. **Enable Two-Factor Authentication (2FA):** Add an extra layer of security to your accounts by enabling 2FA wherever possible. This requires you to provide a second form of verification, such as a code sent to your phone, in addition to your password.
3. **Keep Software Updated:** Regularly update your operating system, web browsers, antivirus software, and other applications to patch security vulnerabilities and protect against malware and cyber threats.
4. **Be Careful with Social-Media: Be** mindful of the information you share on social media platforms and adjust your privacy settings to control who can see your posts and personal details. Avoid oversharing sensitive information that could be used against you.
5. **Beware of Phishing Attempts:** Be cautious of unsolicited emails, messages, or calls asking for personal or financial information. Avoid clicking on suspicious links or downloading attachments from unknown sources, as they could be phishing attempts to steal your data.
6. **Use Secure Websites:** When entering sensitive information online, such as login credentials or payment details, ensure that the website has a secure connection. Look for HTTPS in the URL and a padlock icon in the address bar.