

Basic Digital Safety

Digital Safety: Protecting Yourself And Data Online

within today's digital age, maintaining online safety is crucial. Here are some key practices to ensure you stay secure while navigating the digital landscape:



Use Strong Passwords: using strong passwords is your initial safety precaution. Combine letters (both upper case letters and lower case letter), numerics, and specialcase characters to create a robust password. Try to prevent using easily guessed information like dates of birth or common words



Be Wary of Phishing Scams: Phishing involves tricking people into providing personal information. Be mindful of emails or messages from unknown people asking for sensitive information. You can check the senders email address and look for spelling mistakes as red flags.



Be Cautious with Public Wi-Fi: Public Wi-Fi networks can be a hotbed for hackers. Avoid accessing sensitive information or conducting financial transactions on public networks. Use a Virtual Private Network (VPN) for a secure connection



Keep Software Updated: Regular updates often include security patches. Ensure operating system you use is updated, internet browser upto date, and other critical software are up-to-date to protect against vulnerabilities.

Limit Sharing Personal Information: Be mindful of the data you share online. Try not to post details like your full name, home address, mobile number, and financial information on social media and publicly viewed forums.

Educate Yourself: Keep yourself informed about current online threats and safety practices. information is power when it comes to digital safety. By following these practices, you can masively reduce the risk of falling victim to cyber threats and enjoy a safer online experience. Remember, digital safety is an ongoing process that requires vigilance and proactive measures.



Using Enabled Two-Factor Authentication (2FA): This provides an secondary layer of security. In addition to your password, this will request a second form of identification which could be in the form of a code sent to your phone, to access your account.



Antivirus Software: Reliable antivirus software can detect and prevent malware from infecting your device. Regular scans help keep your system clean.



Regularly Backup Your Data: In case of a cyber attack or hardware failure, having a backup ensures you don't lose important information. Use cloud services or external hard drives for backups.