



DIGITAL SAFETY GUIDE

A GUIDE TO KEEP SAFETY BROWSING USING ONLINE SERVICES



BASIC DIGITAL SAFETY OF EVERYONE

- the whole population now a Days from youngest to the eldest person knows internet and owns a smart device such as mobile phones computers and all the good stuff most people forget about the safety that should be applied browsing the internet that can vary from hackers viruses fake propaganda etc. In these simple steps you and your friends can know how to stay safe and avoid such critical situations

PROTECT YOUR INFO:

☐☐- **STRONG PASSWORDS:** USE PASSWORDS THAT ARE TOUGH TO GUESS. MIX LETTERS, NUMBERS, AND SYMBOLS.

☐☐- **TWO-FACTOR AUTHENTICATION:** ADD EXTRA SECURITY TO YOUR ACCOUNTS.

- Two-factor authentication (2FA) bolsters security by demanding a second verification step, often a code from a mobile app, along with a password, thereby guarding against unauthorized entry. Reference: "Two-factor authentication" (Wikipedia).

According to Wikipedia using a 2FA Verification systems avoid unauthorised beaches by using a notification system and a interactive accepting system by an user this concludes that a strong password isn't the only secure protection system which should be kept in mind about how both of these systems can provide extra protection

Be aware:

☐☐- **pay attention to Phishing:** Avoid entering links or opening attachments from unknown source

☐☐- **Check for verified**

Websites: check that before entering a webpage Look for "https" in the address.

HTTPS is a known form of website that awares users of an safe connection and not a made up link for information grabbers

Secure Devices:

☐☐- **Update your system Software:** Keep your software up to date to guard yourself against attacks.

☐☐- **Use an Antivirus:** Install and keep use of an verified antivirus it will keep your device threat free against virus attack



SAFE BROWSING:

- - **TRUSTED NETWORKS:** AVOID CONNECTING TO PUBLIC WI-FI AS BEING CONNECTED YOUR DEVICE AND YOUR SENSITIVE INFORMATION ARE IN HIGH RISK OF AN CYBER ATTACK IT IS BETTER TO AVOID A PUBLIC WI-FI WITHOUT AN VPN
- - **LOG OUT:** ALWAYS LOG OUT OF THE DEVICE THAT YOU USED TO LOGIN THIS INCLUDES YOUR INTERNET BANKING SOCIAL MEDIA'S AND YOUR EMAILS IT IS AN IMPORTANT OPERATION FOR PERSONAL AND BORROWED DEVICES

- **Smart Social Media Use:**

- • - **Sharing information on social media's** : Don't post too much personal info on social media's as because hackers may take advantage to use your posted information as an valuable asset in their invasion
- • - **Privacy Settings:** browse and select your privacy settings to control who has access to view your information

- **Reviewing Thinking Then clicking:**

- • -**Avoiding to enter Suspicious Links:** Don't click on links from an unknown source to avoid an easier access to your device.
- • -**Safe Downloads:** Only download from trusted websites.

- **Backup Data:**

- Now a days smartphones and smart devices are proposing to their user to create a back up in case their data may be lost it is better to avoid losing your data as smart devices are allowing for a straight forward process to send valuable information to their cloud system

