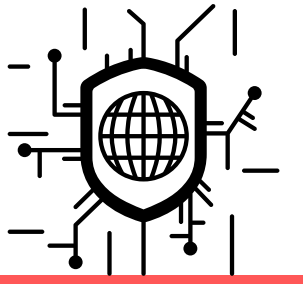




DIGITAL SAFETY: PROTECT YOURSELF ONLINE



ENABLE TWO-FACTOR AUTHENTICATION (2FA).



2FA adds an additional level of security that requires a special code that will be sent to your phone after trying to log in to your account.



USE STRONG PASSWORDS.

Create a password for each resource separately, they should not be similar or identical. Your password must consist of letters, numbers and symbols. Do not use information that is easy to guess or find out, such as your date of birth or your names with the prefix of the current year

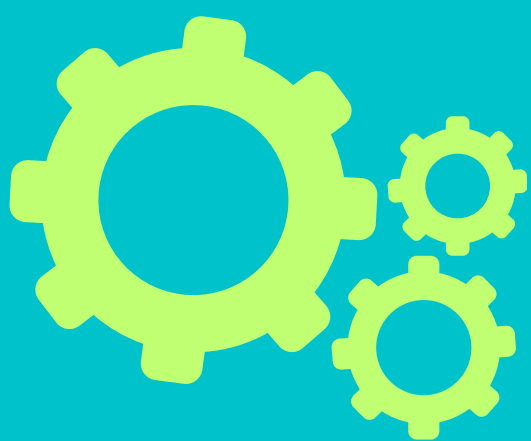


BE CAUTIOUS WITH LINKS AND ATTACHMENTS.

Phishing emails very often deceive users, this is the most popular method among attackers. Therefore, always check the source before interacting.

KEEP SOFTWARE UPDATED.

Always update your devices to avoid data leakage. Turn on automatic updates if possible.



MONITOR YOUR PRIVACY SETTINGS.



Review and adjust privacy settings on social media platforms to control who can view your personal information.



AVOID PUBLIC WI-FI FOR SENSITIVE TRANSACTIONS



Public Wi-Fi is not safe. Use a virtual private network (VPN) to encrypt data when connecting to public Wi-Fi.



THINK BEFORE YOU SHARE.

After you upload something to the network, it will be almost impossible to delete it from the network forever, so think carefully before publishing