Cyber Hygiene

Do's

Use strong and lengthy passwords and change them frequently.

Use privacy settings on your social media accounts and keep them Private.

Lock your computers and mobile phones when not in use.

Enable Two-Factor authentications for your online accounts.

Think before allowing access to Calls, Contacts, messages, Media and Locations while installing mobile applications.

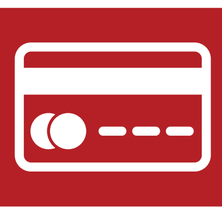
Check for "https:" in URLs before you browse a website.

Remember that UPI pin is used to send the money , not to recieve.

Don’ts

Do not click on the links sent by strangers or pop ups on websites.

Do not answer and furnish your personal information, OTP, Credit/Debit Card information including CVV, to strangers



Do not believe in messages/emails sent to you on mails making false allegations of viewing porn sites.

Do not believe messages requesting money from your friends, relatives, or employers through WhatsApp by seeing DP.

Do not open mail or attachments from an untrusted source.

Do not install unsecured/unverified programs on your computers/mobiles.

Avoid downloading remote applications like any desk or team viewer quick support.

Do not use open/public Wi-Fi networks.

Avoid using charging USB ports at public places for charging your devices.

Do not respond to calls or messages offering part time jobs or work from home.

Beware of fake Trading Platforms before investing in Stocks/IPOs

To report cybercrime, Dial 1930 or login to www.cybercrime.gov.in

TELANGANA STATE CYBER SECURITY BUREAU - TSCSB