Work Place Cyber Hygiene

Saving and scanning any attachments before opening them. Turn off the option: automatically download attachments

Think before you download any apps from unapproved sites

Verify those you correspond with. It is easy for people to fake Identities. Be cautious on possibility of con artists, criminals inside network

Always use High Security settings on Browsers, Networking sites. Keep your Browser, and OS patches and updated

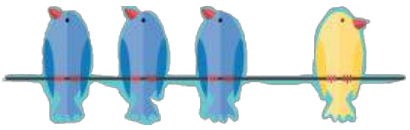
Personally Monitor remote desktop sharing sessions viz. AnyDesk

If you are a victim of Cyber Crime, Dial 1930 & Register your complaint at cybercrime.gov.in

Password Security

Protect yourself, your colleagues, and your employer by using strong passwords

Use Unique Password for unique device



Birthdates make Terrible Passwords

Secure your accounts with Multifactor authentication

Include mix cases, add special characters and punctuation to add strength.

Change passwords periodically

Do not reuse old passwords

If you are a victim of Cyber Crime, Dial 1930 & Register your complaint at cybercrime.gov.in

Mobile Security

Only Install Apps from Official App store to minimize Risk of malware

Backup your data on External Storage medium or cloud at regular intervals. This will allow you to Recover your phone if it gets lost or stolen

Check App Permissions before Installing only grant the permission that are actual required and keep on Eye the Apps that request unnecessary access rights.

Avoid unsecured or unknown public Wi-Fi networks to minimize the risk of data theft and man-in-the-middle attacks.

Make sure that your smart phone always gets the latest updates to close known security gaps

Check your online accounts and services for suspicious activities on a regular basis to detect attacks early on.

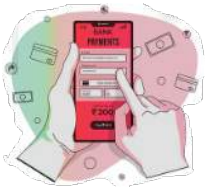
Watch out for suspicious links emails. Don't interact with unknown links and never share sensitive information via email or text message

If you are a victim of Cyber Crime, Dial 1930 & Register your complaint at cybercrime.gov.in

Personal Security

Avoid using Public Wi-Fi for financial transactions

Regular Monitor your bank account activity for any unexpected transactions

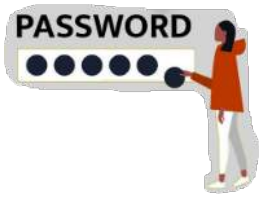


Select the right Privacy settings on social media platforms make sure that you are sharing your information photos and videos with your trusted ones only

Be cautious while accepting chat request from strangers . Your video chats may be recorded and used for blackmailing

Always keep Location service turn off on your device unless necessary

Always secure all your accounts with two-factor authentication, especially while doing any online financial transaction



Never disclose password, One Time Password(OTP), ATM or Phone Banking PIN CVV number etc.,

If you are a victim of Cyber Crime, Dial 1930 & Register your complaint at cybercrime.gov.in

Individual Cyber Hygiene

Think before you download any apps from unapproved sites

Don't open..
The attachment from suspicious or strange sources

Birthdates make Terrible Passwords

Secure your critical information on offline backup drive

Use Unique Password for unique device

Never send Private information, Bank account numbers or passwords in an e-mail

Update your anti-virus regularly & use it to scan your emails

Don't turnoff firewall on your Personal Computer

Install/Update OS security patches from OEM only

If you are a victim of Cyber Crime, Dial 1930 & Register your complaint at cybercrime.gov.in

Employee Cyber Hygiene

- Make your passwords complex. Use a combination of numbers, symbols and letters (uppercase and lowercase) and Change your passwords regularly.
- Do NOT give any of your usernames, passwords, or other computer/website access codes to anyone.
- Do NOT open emails, links, or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization's network.
- Make electronic and physical back-ups or copies of all your important work.
- Report all suspicious or unusual problems with your computer to your IT department.
- If you're leaving it, please lock your computer.
- Update your computer Antivirus software regularly.
- Enable private Browsing or incognito mode.
- Verify websites (check URL of Website "https://" or padlock icon.) Before accessing
- Disable pop-up windows in your browser. Delete browser cookies and cache regularly.
- Always update your web browser with the latest patches.
- Turn on Firewall and Turn off Remote Desktop connections.
- Don't share the folders without authentication

If you are a victim of Cyber Crime, Dial 1930 & Register your complaint at cybercrime.gov.in

Cyber Security Tips

- Keep your software up to date
- Protect your data
- Be careful where you shop online
- Keep your Anti-virus software up-to-date
- Always back up your important files
- Use strong passwords on all devices
- Be careful what you post online
- Don't be an easy target
- Don't use cracked software
- Don't expect anyone to protect it for you
- Never Download pirated Apps/Software as they will often contain malware
- Avoid phishing by watching for urgent tones, unfamiliar senders, poor grammar and suspicious links
- Avoid using public Wi-Fi while doing online transactions
- Avoid phishing attacks Validate the URL for the websites you access before providing your personal data

If you are a victim of Cyber Crime, Dial 1930 & Register your complaint at cybercrime.gov.in