CYBER SECURITY HYGIENE

DOs & Don'ts

DOs COMPUTER SAFETY TIPS

Regularly update Operating System, Internet browsers and Anti-Virus software of the system.

Keep your desktop clean of any sensitive/critical data.

Always maintain regular backup of your critical data in secured environment.

Always keep the desktop/laptops firewall ON.

Dispose computer or hard drive after deletion and wiping of data.

Don'ts COMPUTER SAFETY TIPS

Do not install unknown or unsolicited software on your computer.

Do not use guessable/weak passwords like "password@123" etc.

Do not click on untrusted/unexpected Pop-Up advertisements/ programs.

Do not leave your computer screen "ON" when not in use .

Do not open any Pen drive/portable hard disk without anti virus scanning.

DOs Password Security Management

Always use different passwords for different accounts. Ensure password is strong.

Strong passwords should contain combination of upper case, lower case, numbers, "Special" characters (e.g., @#$%^&*()_+|~--=\’{}[]: ";<>/,etc.)

Immediately, change any password which might have been shared or revealed by mistake.

Change Passwords Periodically.

Don'ts

Password Security Management

Do not use Birth dates, names, ID proofs and other personal information such as addresses and phone numbers while setting passwords .

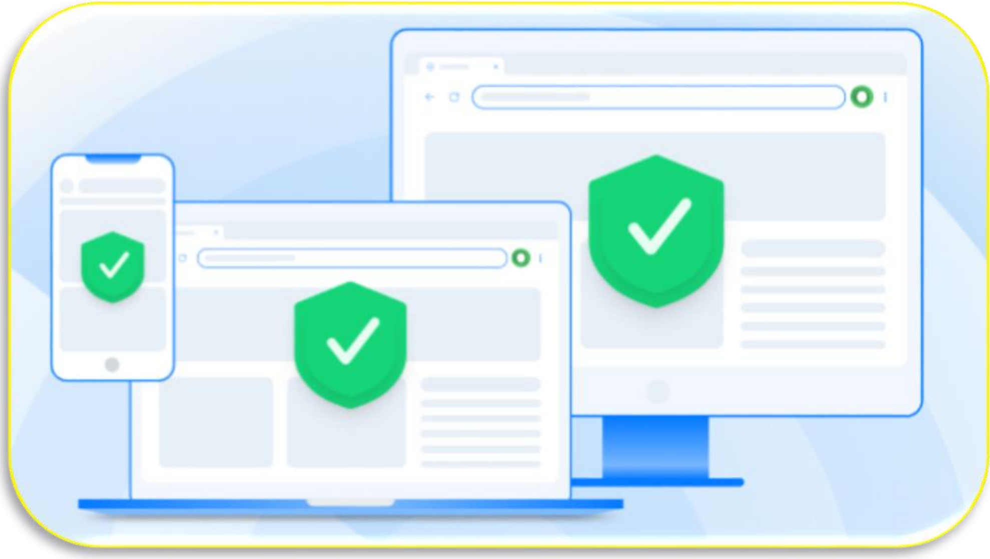
Do not use Common words such as names of family members, pets, friends, colleagues, movie/novel/comics characters, etc as passwords.

Do not use guessable password recovery answers.

Do not create passwords with less than eight characters.

INTERNET SAFETY PRECAUTIONS

DOs



While opening any website look for secured connection by checking if the website starts with "HTTPS" or not.

Be vigilant while clicking/ downloading from suspicious links/ URLs

Make it a habit of clearing browser history after confidential activities/ transactions.

Verify the Authenticity and Identity of social media profiles before getting involved in any correspondence.

Judiciously use services that require location information. Also, avoid posting photos with GPS-coordinates.

Don’ts

INTERNET SAFETY PRECAUTIONS

Do not use any public computer or Wi-Fi for carrying out financial transactions like online shopping, internet banking, UPI transaction, etc.

Do not use email address, phone number and details of payment cards on untrusted and unsecured websites.

Do not trust and share unverified content on social media and messaging apps. Always verify the source and authenticity of content before sharing.

DOs

UPI AND ATM TRANSACTIONS PRECAUTIONS

Keep your UPI PIN safe and do not share with anyone.

UPI PIN is not needed while receiving payments.

Verify the name of “Payee” or QR code before proceeding with the payment

Use cards only after verifying authenticity of PoS/terminals/ATMs and websites

Manage your card limit using mobile banking apps for additional safety

Don’ts

UPI AND ATM TRANSACTIONS PRECAUTIONS

Do not use Public WiFi/Network while doing any transaction / payment.

Do not share confidential information with any one like:-Card Number, Expiry & CVV number etc.

Do not share ATM pin with anyone.

Do not use pirated Operating System for Internet Banking transactions.

DOs

MOBILE SAFETY PRECAUTIONS

Before downloading any App, same should be checked for its reputation/ authenticity.

Protect your device with a strong PIN/Password or Biometrics and enable auto lock setting in mobile phone.

Review the default privacy settings of the smartphone, mobile applications and social media accounts . Personal photos posted on social media with public visibility may be misused .

Be cautious with public Wi-Fi Information shared over public network may be misused.

Don’ts

MOBILE SAFETY PRECAUTIONS

Do not reply or click on link sent through SMS, e-mails or chat messenger by strangers.

Do not log into accounts, especially the financial accounts, when using public wireless networks

Do not store any classified/ sensitive data (text /video / photograph) in the mobile device.