ੴ ਸ੍ਰੀ ਵਾਹਿਗੁਰੂ ਜੀ ਕੀ ਫ਼ਤਹਿ

पंजाब एण्ड सिंध बैंक
(भारत सरकार का उपक्रम)

Punjab & Sind Bank
(A Govt. of India Undertaking)

Where service is a way of life

Cyber Safe: Your Guide To Online Security

HEAD OFFICE CISO CELL

Dear Colleagues,

I wanted to take a moment to emphasize the critical importance of cyber security in our daily operations. In today's digital age, cyber threats continue to evolve and pose significant risks to our Bank's infrastructure, sensitive data, and most importantly, our customers. It is essential that we remain vigilant and proactive in our efforts to protect against these cyber threats. Cyber Security is a collective effort that requires the participation and commitment of every member of our Bank staff. Your commitment to cyber security is vital in maintaining our Bank's integrity and protecting against evolving threats.

Regards,

Dheeraj Kumar Gaur

(Chief Risk Officer)

PHISHING EMAILS

Check for improper spelling or grammar in email content.

Check for suspicious attachments in email.

Avoid sharing financial or Personal information over emails that are not from known sender.

Hover mouse over links mentioned in suspicious email to know the correct address of the URLs.

Check for email content that creates urgency of entering data or clicking on link to do payment or update KYC details etc.

RANSOMWARE

How Ransomware Infection Occurs ?

Visiting Suspicious Websites / Opening Phishing Emails

System Infected / Files Encrypted and Demand of Ransom

Data Lost

What to Do if infected ?

Disconnect the System from Internet

Report the Incident To Concerned Authority

Restore Data From Backup To Clean Device

Backup Data Regularly

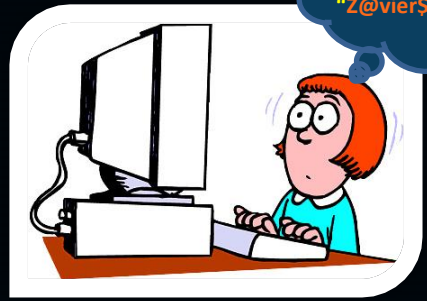
Keep Antivirus and Windows Updated

Do not Open Suspicious Emails

Do Not Click Suspicious Links on Websites

Guidelines For Strong Password

- Create password having combination of Capital letters, small letters and special characters.
- Never use words from dictionary or personal information as your passwords.
- Use 2- Factor authentication wherever possible with passwords.
- Change your passwords regularly and try to use different passwords for different accounts.



Never use default passwords like Admin@123, Password@123 or 123456

The more complex the password, the more difficult it is for the hacker to unlock it.

Guidelines For Browsing Internet Safely

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

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

While sharing any picture on any website make sure it does not disclose your location or GPS coordinates.

Do not share any personal information over email or any social websites with strangers that you do not trust.

Mobile Device Safety

Review the default privacy settings of the smartphone, mobile applications and social media accounts .

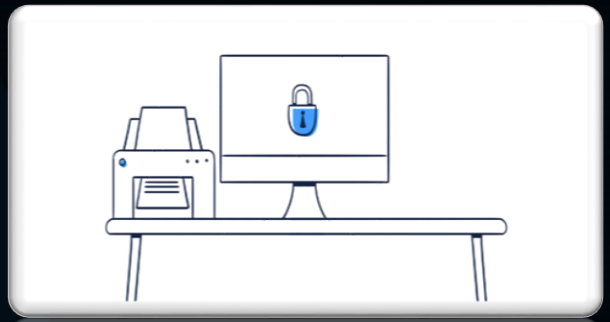
Protect your device with strong PIN/Password or Biometrics and enable auto lock setting in mobile phone.

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

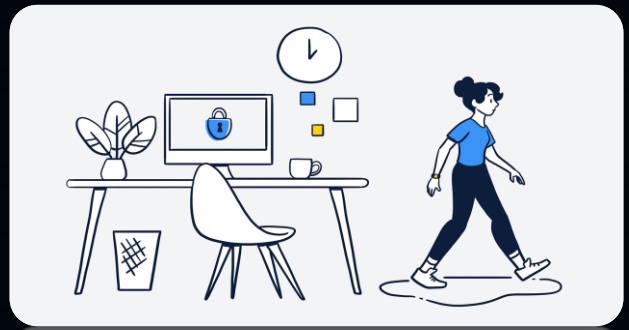
Do not store any classified/ sensitive data (text /video / photograph) in the mobile device.

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

Clear Desk & Clear Screen Policy



- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- Computer/ workstations must be locked when workspace is unoccupied.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Computer/ workstations must be shut down at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.



Guidelines on Day To Day Activities of the Bank

AD ID/ Finacle Password must not be shared with anyone.

Make sure to log out from Finacle or Email account whenever the system is not is use.

Passwords must be changed regularly and must be complex in nature including Capital/Small letters and special characters.

Make sure the confidential information of customers like account statement, loan documents etc that are printed should not be kept in open and must be stored in lock and key.

Do not click on links and URLs received in email received from unknown user .

No sensitive information like account statements, loan statements must be placed on Desktop screen .

Desktop/System must be locked when leaving the system by pressing the shortcut keys “Windows + L”.