"BASIC CUSTOMER AWARENESS FOR CYBER SECURITY"

A. Automated Teller Machine (ATM)

Steps to be taken care while using ATM

1. **Do not give your PIN number to anyone over the phone.** Thieves often steal cards and then call the victims for their PIN, claiming to be law enforcement or from the issuing bank.
2. **Use an ATM located near the center of a building.** Always pay close attention to the ATM and your surroundings. Don't select an ATM at the corner of a building — corners create a blind spot.
3. When leaving **an ATM make sure you are not being followed.** If you are, drive immediately to a police or fire station, or to a crowded, well-lighted location or business.
4. Do not allow **people to look over your shoulder as you enter your PIN.** Memorize your PIN; never write it on the back of your card. Do not re-enter your PIN if the ATM eats your card — contact a bank official.
5. **Do not wear expensive jewelry or take other valuables** to the ATM. This is an added incentive to the assailant.
6. **Closely monitor your bank statements,** as well as your balances, and immediately report any problems to your bank.
7. **Try to use the same ATM consistently;**

8. **Always inspect the ATM & make sure it doesn't look different than before.** If it does, don't use it - and alert your banking institution;
9. Be wary of those trying to help you, especially when an ATM "eats" your card. They may be **trying to steal your card number and PIN**
10. **Never Speak you pin while you are using ATM machine**

B. Mobile Banking

Steps to be taken care while using Mobile Banking

1. **Never store your account information,** such as the account number, debit and credit card PINs, **on your mobile handset.**
2. **Use a banking app, never store your user name and password on your mobile handset for automatic login.** This may allow faster access, but is a potential hazard if the mobile falls in wrong hands.
3. **Never use mobile banking when you are on a public network, including free WiFi hotspots.** Always use your mobile service providers network or a password- protected WiFi connection.
4. Never **send your account information via text message.**
5. **Set a screen unlock pattern,** a number based or a text-based password.
6. **Be careful while downloading App.** Review & ratings are to be checked before downloading any app from Playstore because they can bring Malware.
7. **Don't click on malicious links** i.e. Got a mail inviting you to click on your bank's website? Don't fall for it because it could be a fake website designed to mimic your bank's official site. Never follow a banking link sent to you in a text message or e- mail.

8. **Use Social Media Sites judiciously** like Facebook etc. Users get trapped when they share sensitive information to scammers.
9. **Be aware of unsolicited calls** asking for sensitive information like OTP, PIN etc.

C. Internet Banking

Steps to be taken care while using Internet Banking

1. Use Only Secure Wi-Fi Networks
2. Use only those Banking sites which has “https” in their URL Address
3. Enable Two-Factor Authentication i.e. User Password & OTP
4. Disable Automatic Login Before Logging in to your Account. Always login a fresh and do not store your credentials in cookies
5. Beware of Phishing Calls, Texts and Emails asking for sensitive information like Password, OTP and other such details
6. Create a Strong Password having minimum 8 digits with Alpha, numeric, special character, Upper & lower case and difficult to guess
7. Use Antimalware (or Antivirus) Software on your computers to detect latest virus
8. Use only Official Banking Apps/website while performing transactions.

D. Website & Internet Usage (Personal & Professional)

Cyber Security Tips
DON'T BELIEVE EVERYTHING YOU READ.
Be cautious about what you receive or read online—if it sounds too good to be true, then it probably is.
NCC

Steps to be taken care while using any Website/Internet

1. **Always change your default passwords**, for each of your accounts, and change them at least once a month to keep your personal information safe;
2. **Use multifactor authentication** whenever possible, as well as secure passwords, to confirm your identity when you log into your accounts;
3. **Be sure to keep your operating system, browser, and other software up-to-date** with security patches to minimize threats from viruses and malware;
4. **Limit what you do over public Wi-Fi** and use software that creates a secure connection over the internet such as a Virtual Private Network (VPN) to safely connect from anywhere;
5. **Practice safe surfing and shopping**, checking that the site's address starts with "https", instead of just "http";
6. **Enable privacy settings** and increase the default security settings of the software you use;
7. **Be selective when sharing personal information** as this could be used by hackers to guess passwords and logins;
8. **Do not downloaded pirated software**, as it is not only illegal, but almost always includes some type of malware;
9. **Back up your data**, Use an external hard drive, as this is the easiest way to recover from a ransomware attack.

****