Safe and Responsible Banking Usage Guidelines

Whether it is Mobile banking or internet banking, withdrawal from the branch or the ATM, one needs to take care and observe some basic precautions to ensure a safe banking experience. We, at Equitas Small Finance Bank (ESFB) believe in the practice of Safe Banking. It begins with making sure that your contact details are updated in our database so that the alerts don't go unintended recipients. In case you are travelling overseas, ensure that your email ID is registered with the bank.

List of Do's and Don'ts:

Beware of fraudsters who target you through calls/ SMS/ Emails under the pretext of updating your KYC details as your account/card is blocked, availing an increased credit card limit, earning cashback points/rewards or availing a loan/top-up on a loan. Do not fall prey to such scams.

Do not fall prey to such scams.

Here are the DO's and DON'Ts to protect yourself and stay safe online:

Do's

- Always visit the official website for the Bank's contact details
- Always keep your contact details updated with the bank and subscribe to get transaction alerts
- Install genuine anti-virus and anti-malware software on your computer/mobile and keep it up-to-date
- Keep your password strong and unique
- Turn off your browser's autocomplete settings to avoid storing your card number, passwords or any other personal/sensitive information
- Be careful before downloading any apps from Play Store or App Store
- Look for the padlock sign or https in the status bar of your web browser while transacting
- Always look out for spelling errors in messages that ask to share sensitive details, as they will help you identify the fakes.

Don'ts

- Never share sensitive details like PIN, passwords, OTP or card details with anyone
- Avoid using public Wi-Fi or free VPN/public computers while accessing your Bank account
- Do not click on links received from unknown sources/sender IDs
- Stay away from commonly used passwords like 123456, Names, Birthday etc.
- Avoid writing your Banking password anywhere and saving it on browsers
- Do not download remote sharing apps e.g. Anydesk
- Do not scan a QR code or enter a PIN or OTP to receive money through UPI
- Do not take help from strangers at the ATM

Remember:

ESFB or its employees/representatives will never ask for your personal account information.

1. Password Protection

Hackers are aware that people use the same or similar passwords for multiple accounts. If your banking password, Amazon password, and email password are the same, then a vulnerability in one site can put others at risk.

What makes a password easy to guess?

Once hackers acquire a list of email addresses from a data breach, they already have a good start. From there, they simply have to pick a website of their choice and try the enlisted emails with the most popular passwords. There are chances of getting into quite a few accounts.

To avoid your account from getting hacked, here's a list of worst passwords you should avoid:

- Avoid using 123456, the most common of all passwords.
- Switching a letter to a symbol like p@ssw0rd! too is an obvious trick that hackers know. Password cracking programs contain every type of these combinations in every language.
- Use something obscure and avoid using names of your favourite sports team or pop culture references.
- Using single words like sunshine or monkey and adding a number or punctuation at the end, doesn't make for a strong password. Instead, use a phrase or sentence to make your password stronger.
- Avoid using common patters like 111111, abc123 or 654321.

What makes a password strong?

- Combining unrelated words.
- Using an entire phrase and changing some of the letters to special letters and numbers.
- Use a combination of upper and lower case letters, symbols and numbers.
- The longer your password, the stronger it is.
- Use different passwords for every account.

2. Debit Cards

Here are a few 'Dos and Don'ts', which will help you to avoid debit and credit cards frauds and enjoy a safe and hassle-free banking experience.

Dos

- Upon receiving the welcome kit, ensure that the envelope is sealed. If there is any hint of tampering, contact the bank immediately.
- Immediately sign on the reverse of the card.
- Change the PIN of the card after receiving it. Ideally, do so every six months for complete protection.
- Keep your cards safely. In the case of loss or theft, immediately inform the bank.
- After receiving a new or upgraded card, discard the old one by cutting it diagonally.
- It is advisable to change the PIN after an overseas trip.
- Try and memorise your PIN instead of writing it anywhere.
- Avoid using physical keyboards and preferably use Virtual Keypad (show image) to input your credentials in your lap top or mobile.
- Be careful while entering your PIN anywhere – ATM, card machines, etc.
- Update your email and phone number for constant alerts on any card activity. Keep an eye on your transactions and purchases and report any unusual transactions to the bank immediately.

- Make sure that you have the 3D secure for your cards, in the form of Verified by Visa (VbV) or Mastercard Secure Code (MCSC). This is a mandate for online transactions now and all ESFB cards have it.
- Always check the url of the website to make sure that it is a secure one before making the payment. Quick check: make sure there is a lock icon (https://show lock symbol) on your browser, which indicates that the website is using an encryption technology while transmitting sensitive data. On clicking the lock you can see the digital certificate and other details related to the website. Proceed only if such verification is available
- Check the url of sites if it displays the IP address or numerical address instead of domain name as such sites are likely to not be a genuine site.

Don'ts

- Remember that Equitas Small Finance Bank will never ask you for details such as a copy of the front and back of your card.
- If anyone claims to be a bank representative and asks for your card, do not hand it over.
- Never share your card details like card number, expiry, CVV, PIN or OTP with anyone, even if they claim to be bank officials.
- Do not saving your card details on online merchant websites.
- Never enter your details on emails with input fields asking for your cards details, ATM PIN, CVV, UPI PIN etc
- Avoid using your cards on unauthorised payment gateways such as those of gaming websites, pornography websites, lottery, gambling, and more.
- Never sign a blank application form with the promise of it being filled later on by the bank representative.

3. UPI

Do's:

- Download UPI application through valid platforms i.e. Google Play store etc.
- Register for mobile banking through your base branch/net banking/UPI.
- Make sure you login and initiate UPI transaction in complete privacy.
- After completing transaction, make sure you logged out of application successfully.
- For every transaction, you will receive sms alert to your registered mobile number. If you find any unauthorized UPI transaction in your account, please take up with your branch immediately.
- In case of any failed transactions, please take up with escalation matrix provided on website and application.
- Change your UPI application password and UPI PIN / MPIN frequently.
- In case of unauthorized access of your mobile banking/UPI, please de register immediately through ATM / internet banking / base branch (or please contact our Contact Centre).
- In case your mobile phone is lost / stolen, please de register your mobile banking immediately through Base branch / Net banking / ATM / contact center.
- In case your mobile banking / mobile number is de registered / deactivated without your request or you get a call in this regard, somebody may be trying to get a duplicate SIM/ steal your credentials like mPIN / OTP (One time password), etc. In this case, please contact your base branch immediately.

Don'ts:

- Please do not share your passwords / do not store it in your Mobile handset.
- Never let anyone see you entering your application password or UPI PIN / MPIN.
- Never use application/ UPI PIN / MPIN that can be easily guessed Ex: 1111/2222/1234/ Birth year, mobile number/telephone number.

- Don’t install and use UPI application in someone else device.
- Equitas bank does not make calls / emails, asking for your UPI / Mobile banking passwords. If any caller pretends to be from our Bank / Contact Centre, please do not entertain such requests as they are fraudulent entities.
- Never carry your registered SIM card and debit card together, as there is a risk of losing both of them, which may enable anybody gaining access to your account.