Aditya Birla Idea Payments Bank Limited - Security Tips

10 Golden Rules for Security

1. Change your password regularly

• Change and memorize your PIN, password and other security information received by you on at regular intervals. More importantly, keep the password confidential & Change periodically.

2. Always use strong hard-to-guess passwords

- Do use hard-to-guess passwords or passphrases. A password should have a minimum of 8 characters using uppercase letters, lowercase letters, numbers and special characters.
- Don't use passwords that are obvious, like your name, surname, family members, mobile number, DOB or common works like "password," "Newuser123," or obvious character sequences on the keyboard, like "asdfg" and "12345678."
- Use the Virtual Keypad for enhanced security while keying in your Internet Banking passwords
- Disable 'Auto complete' and remember password feature on the computer

3. Do not share your confidential details with anyone

- Your privacy and security are very important to Bank. Bank will never contact you via email or text message requesting that you verify your Bank Online User ID and Password, Number, Debit Card, Credit Card, PINs, or other confidential personal or sensitive account information.
- Do not respond to emails or phone calls requesting confidential /Personal details on behalf of Bank. Kindly note that the Bank will never ask for details about your Account / PINs or Passwords
- Do not post any private or sensitive information, such as debit card numbers, passwords or other private information, on public sites, including social media sites

4. Do not leave sensitive information/Document lying around unattended /public space

- Do not leave printouts containing private information unattended. It's very easy for a fraudster to glance down and see sensitive documents.
- Do not throw confidential data in open trash containers without destroying it completely.

5. Be cautious of suspicious emails and links

•

• DO NOT open mail or attachments from an untrusted source. If you receive a suspicious email, the best thing to do is to delete the message, and report it Bank. Even opening or viewing these emails and links can compromise your computer/Mobile and create unwanted problems without your knowledge.

• DO NOT click on links from an unknown or untrusted source. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage networks. • Type your internet banking URL. It is a safer to type bank URL than clicking on links given in an email.

6. Always Lock your computer and mobile phone when not in use

- Always lock your computer and mobile phone when you're not using them.
- Always logout to terminate your session, instead of closing the browser applications directly

- Do lockout your computer and mobile phone when not in use. This protects data from unauthorized access and use.
- DO Not leave your devices unattended in public area. Keep all mobile devices, such as laptops and cell phones physically secured.

7. Do not install any unauthorized programs

• Do not install any unauthorized programs on your computer/Mobile. Malicious applications often pose as legitimate programs, like games, tools or even antivirus software.

8. Do not use public computers for banking

• Avoid using PCs installed in public/open areas to access Internet Banking. If you have to login from such places, ensure that you clear the cache and browsing history, and delete the temporary files from the public computer.

9. Subscribe for mobile notifications

• If you haven't done it already, do it now. These notifications will alert you quickly of any suspicious transaction. Always ensure whether the right amount has been deducted from your account. If you see any discrepancies in the amount, inform the bank immediately.

10. Stay alert and report suspicious activity

• Always report any suspicious activity to the Bank. It's our responsibility to stop cyber-attacks and to make sure our data isn't lost or stolen. All of our jobs depend on keeping our information safe. In case something goes wrong, the faster we know about it, the faster we can deal with it.

Misuse of Logos of Commercial Banks by Fraudulent Websites

Aditya Birla Idea Payments Bank Limited advices the public to stay alert of various entities which operate websites/ make calls claiming to represent the bank and promise to enlist individuals as Customer Service Points (CSP) for the bank. Such fraudulent websites display the logos of various prominent commercial banks, collect varying amounts from interested individuals to open CSP and subsequently dupe them. Beware of such fraudsters and do not engage with such entities as they are unincorporated bodies and not registered with RBI.