Customer Security Tips

Customer Security Tips

Mobile Security Precautions

Do's

1. Password protect the mobile phone and never give your mobile phone to anyone.
2. Choose a strong password to keep your account and data safe.
3. Review your account statements frequently to check for any unauthorised transactions.
4. Change your PIN regularly.
5. Report a lost or stolen phone immediately to your service provider and law enforcement authorities.

Don'ts

1. Never give your PIN or confidential information over the phone or internet. Never share these details with anyone.
2. Don't click on links embedded in emails/social networking sites claiming to be from MAFIL or representing MAFIL.
3. Don't transfer funds without due validation of the recipient, as funds once transferred cannot be reversed.
4. Don't store sensitive information such as credit card details, mobile banking password and user ID in a separate folder on your phone.
5. Don't forget to inform MAFIL of changes in your mobile number to ensure that SMS notifications are not sent to someone else.
6. Never reveal or write down PINs or retain any email or paper communication from MAFIL with regard to the PIN or password
7. Be cautious while accepting offers such as caller tunes or dialer tunes or open/download emails or attachments from known or unknown sources
8. Be cautious while using Bluetooth in public places, as someone may access your confidential data/information
9. Be careful about the websites you are browsing. If it does not look authentic, do not download anything from it.
10. Do not share copies of KYC documents with unidentified persons, unverified/unauthorized Apps. You are requested to report such Apps/Bank Account information associated with the Apps to concerned law enforcement agencies or can file complaint using Sachet portal through below link

    https://sachet.rbi.org.in/Complaints/Add

Secure Phone Banking

1. While talking to the Phone Banking officer, never disclose the following:
    - 4 digit ATM/IVR PIN
    - OTP
    - Net Banking password
    - CVV (Card Verification Value
2. Ensure that no one see you entering you PIN (personal identification number).
3. Avoid giving verification details to the Phone Banking officer while in public places.
4. The Phone Banking channel is meant to be used by the account holder only. Do not transfer the line or hand over the phone to any other person after you complete self-authentication.

Secure Computer Usage

1. Use licensed software. Software purchased from untrustworthy sources could have virus or trojans that could corrupt your files and reveal your confidential data.
2. Protect your computer accounts with strong passwords
3. Update your computer with latest security patches for your operating system, browser and email client.
4. Use anti-virus, anti-spyware and personal firewalls

Creating Safe and Secure Passwords – Do's

1. Keep alphanumeric passwords that are at least 8 characters long. Mix upper and lowercase letters, and special characters like $, @, *, etc.
2. Be creative and think of a password that is really different as well as difficult to guess. You can use phrases in sentences such as "nature's wrath tsunami" to frame your passwords as they are easy to remember and difficult to crack.
3. Place punctuation or numbers randomly.

Don'ts

1. Don't use dictionary-based words, your spouse's name or your date of birth. These are easy to crack or guess.
2. Don't use sequences of letters or numbers. E.g.: abcd1234. asdfg123 etc.
3. Do not keep the same passwords for multiple accounts. Once hackers have guessed one password, they'll often try to see if it works on other accounts.
4. Do not write down your passwords.
5. Don't use personal information like your name, date of birth, PAN number, etc.
6. Change your passwords once in every three months.

Protecting Your Password

1. Memorize your PIN. Don’t write down your password or PIN anywhere especially not on your card.
2. Change your PIN/passwords at regular intervals.
3. If you suspect that someone knows your PIN/Password, change it immediately.
4. Don’t send your password or PIN to anyone via email or text message.
5. Don’t say your password or PIN aloud in public where other people can hear you.
6. Don’t have your browser remember your card/account password.

Secure Internet Browsing

1. Observe click discipline while browsing through different websites. You may land up clicking on to malicious link that could download malicious code / software or virus on to your computer.
2. Downloading software from non-trustworthy sites including torrent sites may lead to infecting your computer with virus.
3. Read privacy policy of the website before entering personal information such as name and email ID. Be aware of how your information would be used by the website owner.