Tips To Protect Your Mobile Device

As Mobile Banking becomes part of banking convenience on the go, securing your mobile device has become as important as protecting your computer. Here are some precautionary measures you can take to keep your mobile devices protected:

1. **Secure your device with a password**
   a. Create a strong password for your mobile device that is easy to remember, but hard to guess.
   b. Set your mobile device to lock automatically when not in use.

2. **Download secure applications**
   a. Download and install reliable antivirus software on your mobile device
   b. Keep any security patch and antivirus software up-to-date.

3. **Exercise cautious when downloading applications**
   a. Before you download any new application, do check the ratings and comments to be aware of what the app does and what information it may access on your mobile device.
   b.
4. **Delete old messages**
   a. Do delete text messages from your financial institution after reading them as such information may lead to identity theft.

5. Do not “root” or “jailbreak” the smartphone, as this could compromise smartphone security.
6. Do not download applications from unauthorised or illegitimate app stores, or random download locations on the internet. Do not click on hyperlinks from messages, emails if you are unsure of the source.
7. Be alert especially if a screen on your mobile device suddenly pops up and asks for your confidential information, even if you did not open your applications or initiate any activity.
8. As cybercriminals’ mode of operations and malware could constantly be evolving, visit your bank’s websites for more information and latest updates on other signs to watch out for.
9. If there is an update for your device from legitimate sources such as Google Play Store, or Apple Play Store, install it. New updates are sometimes used to fix bugs and address security vulnerabilities.

What are some of the symptoms of mobile malware infection?

- **Bad Battery Life:**
  Whether malware is hiding in plain sight, pretending to be a regular application, or trying to stay hidden from the user, abnormal battery drainage can often give away the presence of an infection. This could be due to malware utilising the system resources to perform its actions (e.g., communicating with a command and control server) in the background.
- **Dropped Calls and Disruptions:**
  Mobile malware can affect outgoing and incoming calls. Frequently dropped calls or disruptions during a conversation could be the interference of mobile malware. Call your service provider to determine if the dropped calls are its fault. If it’s not, it is possible that someone or something is trying to eavesdrop on conversations or perform other suspicious activities.
- **Unusual Phone/Data Bills:**
  Android malware often infects devices and starts sending SMS text messages to premium-rated numbers. Some malware may send an SMS message just once a month to avoid suspicions, or they may uninstall themselves after causing unusually large mobile/data bills. Malware can also smuggle, steal and send sensitive data from your device to a third-party. Significant changes in your download or upload patterns could be a sign that someone or something has control over your device.
- **Clogged Performance:**
  Malware infection may cause serious performance problems as it tries to perform unauthorised activities in the background such as read, write or sending data from your smartphone. Checking RAM (Random Access Memory) use or CPU load could reveal the presence of malware that’s actively running on the device.
- **Suspicious Applications:**
  If you notice an unusual change in the look-and-feel of your smartphone (such as new icons or applications), malware may have infected your phone