Suspicious SMS & calls

Dos

- ✓ Check the sender's number or identity if a SMS is received.
- ✓ Check with the bank about the content in the SMS.

Don'ts

- ✗ Reply to any SMS and give your card details or account details.

Install a Virus Guard

Dos

- ✓ Install a well-recognized virus guard.

Don'ts

- ✗ Turn off your virus guard in any case.

Update the system & anti-virus

Dos

- ✓ Keep the devices up to date.
- ✓ Keep the Operating systems and virus guards updated.

Hithawathi

"The main objective of Hithawathi project is to provide assistance and guidance on cyber issues to all Sri Lankan citizens, especially women and children. Moreover this makes the society aware of how to stay safe in cyberspace with necessary safety tips, knowledge and security information through Hithawathi website, social media channels and printed materials.."

"Hithawathi", which provides all these services for free is another social project carried out by LK Domain Registry.

Contact us

011-421-6062 help@hithawathi.lk +94 77 771 1199

Business Hours

Weekdays 08.30 am – 07.00 pm

Saturdays 08.30 am – 05.00 pm

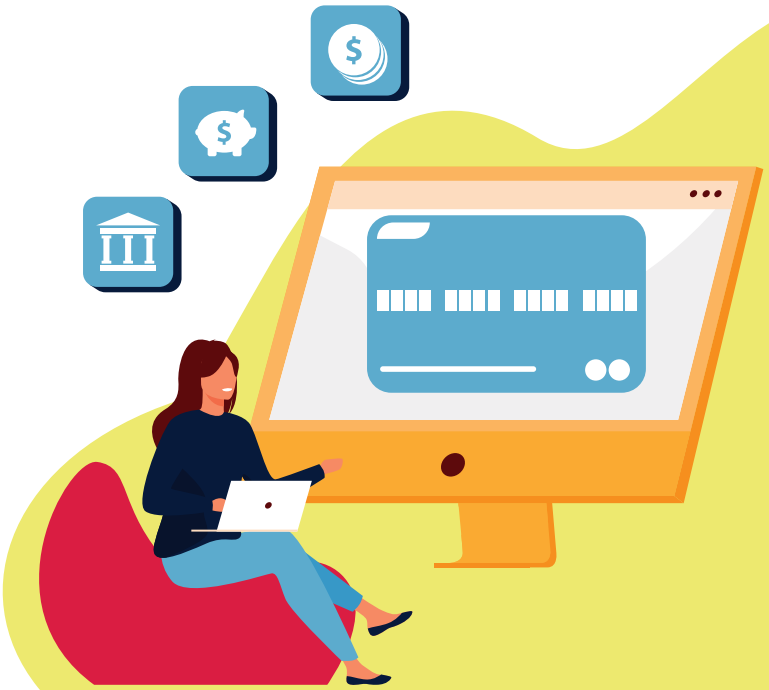
Closed on Public holidays.

© Copyright - Hithawathi

හිතවති | ஹித்தவதீ | HITHAWATHI

Safe Banking

From Hithawathi



www.hithawathi.lk

Password..

Dos

- ✓ Create strong passwords.
- ✓ Enable Multi-Factor Authentication (MFA) whenever possible.
- ✓ Save passwords in secured password managers.

Don'ts

- ✗ Write passwords on papers.
- ✗ Share One Time Password (OTP) with others.
- ✗ Use the same password for every account.
- ✗ Use a password which is easy to guess like Birthday, NIC number or a phone number.

Device

Dos

- ✓ Use a strong security method to unlock like fingerprint, a pin or a password.
- ✓ Keep the devices locked when not in use.

Don'ts

- ✗ Keep logged into the banking apps or banking sites when not in use.
- ✗ Jailbreak or root the device.

Login Process

Dos

- ✓ If you feel that someone is peeping in to your activities with your banking app, immediately change the passwords.

Don'ts

- ✗ Allow someone else to log into your banking apps and accounts.

Connectivity

Dos

- ✓ Always use a secure connectivity.

Don'ts

- ✗ Log into the online banking app via a public Wi-Fi connection.
- ✗ Use a public / shared computer to log into online banking portals.

Apps & Software

Dos

- ✓ Be cautious when downloading and installing mobile applications.
- ✓ Check the access permission requests and the source of the app.

Don'ts

- ✗ Install apps from unknown providers / third party sources.

Links & Websites

Dos

- ✓ Carefully check the URLs (links of websites) received via any e-mail or a message.
- ✓ Double check with the bank if you receive any e-mail mentioning anything about your bank.

Don'ts

- ✗ Click on the links received through e-mails and social media.
- ✗ Provide your card details or credentials to any unknown link or an interface.

Check security of websites

Dos

- ✓ Check the website's URL before paying whether it is https:// instead of http://

Don'ts

- ✗ Ignore security alerts.