Deutsche Bank AG, Colombo

We would like to bring to your attention a noticeable increase in cybercrimes in Sri Lanka within the recent past. Cyber criminals are using increasingly sophisticated methods to target individuals and businesses including phishing emails, fraudulent links, identity theft and unauthorized access to financial accounts. The most important thing is to protect your passwords, account details, etc. Be prepared to protect yourself against cybercrime.

Protect your private information.

- Implementing a “clear desk policy” can reduce the risks at your workplace – risks such as password hacking, handling confidential documents or misappropriation of information and content, particularly by company employees or visitors, can be minimized
- Confidential information must not end up in the wrong hands. Documents and data should be classified correctly so that all information is handled properly during its usage (e.g. creation, access, changes, transmittance, and storage)

Protect your emails

- Delete spam email and on no account open any links and attachments in such emails
- Use the “forward” instead of the “reply” function and enter the correct email address manually. This way you can ensure that the email and its contents do not end up in the wrong hands
- Check any requests that are claiming to be urgent as these may be bogus and verify them with the alleged sender before taking any action

Create a “human firewall”

- Organize cyber security awareness training for your employees
- Keep your employees informed of the latest fraud trends and protection measures available, e.g. by sending out a regular newsletter
- Carry out tests to identify social engineering and phishing

Safeguard your computer

- Do not download any files from unknown sources from the internet or from a USB stick
- Ensure that your computer has the latest malware-antivirus protection and that the latest security updates have been installed
- Set the macro security settings to the highest possible level
- If possible, use a separate computer with special physical safety controls for making online payments
- Use different passwords for different systems, update them regularly and delete inactive accounts

Protect yourself against the risk of making incorrect payments

- Use the dual verification principle for authorizing payments above a certain amount
- Use 2-factor authentication for authorizing payments
- Check your payment accounts daily
- Implement threshold value monitoring for unusually large payments
- Where possible, use 2-factor authentication for your customer login
- Create a whitelist of valid payment accounts
- Make sure that the various tasks associated with the recording, confirmation and approval of payments are properly separated from each other

May 2026