Internet and Banking Security

January 2021

Internet and online banking applications are popular targets for fraudsters. To protect your account and personal data, we recommend the following security measures:

Online banking
- Avoid using public computers or public WLAN connection to do online banking as it could be intercepted
- Only login to online banking via the LGT website. If you use the LGT mobile banking app, be sure to download the app from the official app stores.
- Never disclose your user IDs, passwords or activation letters to anyone including LGT staff.
- Keep your login credentials and devices secure and protect them against wrongful use by unauthorized persons.

Device security
- Use the latest release of all operating systems and browsers on all devices (computers, laptops, cell phones, tablets, etc.).
- Minimise cybersecurity risk by installing up-to-date virus scanner, effective firewall, mobile hard drive encryption, etc.
- Always lock your device or log off if you have finished using it.

Password security
- LGT online banking users should change any passwords provided to them by LGT immediately upon receipt and destroy the original printed copies of the passwords.
- Choose a unique password for online banking and do not use it for other services or websites.
- Passwords should be complex (e.g. combination of upper and lower case letters, numbers and symbols) and must not contain easily accessible personal information, e.g. telephone number, date of birth, part of a name, etc.
- Passwords should be changed regularly.

Recognize phishing emails
- Analyse e-mails carefully to spot phishing attempts. Even an email that seems to come from a familiar sender could be forged. Common signs of phishing emails:
  - Generic greetings;
  - Poor spelling and grammar;
  - Requesting for personal information such as credit card number, passwords, etc.;
  - Urgent actions required;
  - Unusual requests such as transferring money to an unknown recipient;
  - Suspicious attachments or links; etc.
- Be cautious and never click on links / open attachments / reply if the email seems suspicious.

Stay vigilant
- Always use secured and trusted wireless network.
- Add a password to your home Wi-Fi network.
- Beware of phishing scams:
  - Always question unsolicited or unexpected contacts purporting to be from LGT.
  - LGT will never ask you to disclose confidential information such as your online banking password, account details, etc., via phone calls, emails or SMS messages.
  - LGT will never grant remote access to your online banking by telephone or e-mail.