SECURITY

Bank Leumi takes online security very seriously.

We place the highest priority on your online security to ensure the confidentiality and security of your financial information and transactions and are constantly reviewing our infrastructure and security measures, such as firewalls and encryption technology to ensure they're up to date and meet our stringent security requirements.

Data encryption Our Online Banking service is hosted on a secure, encrypted server. This means that any information you send us is encoded for your protection so that your personal login credentials are not visible to anyone who might attempt to steal your identity.

Timed log out Online Banking logs you out after 5 minutes of inactivity. This gives you added protection if you forget to log yourself out.

Deactivation of your login details We will automatically disable your access to Online Banking if three incorrect attempts are made to log in using your details. This is to stop fraudsters making repeated attempts to get into your account.

Debit Card Security As of January 2020, we have upgraded our debit card offering and there is now a 24/7 fraud check in place. If we suspect a fraudulent transaction may be in progress, we will send a text message to the cardholder asking them to call the fraud hotline.

A dedicated telephone number – **0333 241 6947** – has been set up for this purpose (separate from the Leumi UK helpdesk number). This is a **24-hour service**.

Tips for protecting yourself against fraud

- Never login to your bank website through a link in an email, even if the email appears to have come from the bank. BLUK will never send you an e-mail, text or website link asking you to enter your personal details and passwords.
- The login pages of our website are secured through an encryption process, so a locked padlock will appear in your browser window when accessing your bank site.
- Be wary of any unexpected or suspicious looking pop-ups that appear during your online banking session.
- Stop and think about the process you normally go through to make a payment to someone – be suspicious if it differs from the last time you used it.
- Never give anyone your login details in full either by email or over the phone – we will never request these in this way.
- Do not open unsolicited emails with attachments. These may contain a virus.
- Browsers often come with security features built in. Make sure they are activated and keep your internet browser up to date.
- Maintain and monitor your own hardware and software to ensure that it is not contaminated by malware and viruses.
- Ensure that you have up to date anti-virus software installed on your computer, together with up to date software, including Adobe if you use it. Always check for the latest updates and install them.
- Check your bank statements regularly and contact the Helpline or your Relationship Manager immediately in the unlikely event you spot any transactions that you didn't authorise.

For further information about securing your computer visit: https://www.getsafeonline.org/protecting-your-computer/ which is a third party resource from Get Safe Online that provides guidance and practical advice on how to protect yourself against fraud, identity theft, viruses and other problems encountered online.