03.03.2022

How to drive bank fraudsters absolutely insane

Cyber criminals are continually coming up with new methods to get their hands on their victims' money. In the light of this, here's a recommended video which uses a large dose of humour to call attention to a current threat.

Despite the entertaining tone of this video, it addresses a rather current method employed by cyber-criminals – but see for yourself: www.youtube.com/watch?v=8_5eQw-kdyM (http://www.youtube.com/watch?v=8_5eQw-kdyM)

You can protect yourself against the risks involved in entering a financial institution's address into a Google search window to access your e-banking portal with the following measures:

- Always enter the address manually and directly into your browser address line – not into the Google search window!
- Never type "my bank log-in" or "e-banking my bank" or similar into the Google search window. Google shows you adverts (even those of fraudsters!) before displaying actual search results. Never click on any such ads in case they mention your financial institution.
- Make sure you are using a secure connection (with a lock symbol, the correct financial institution's name and the correct domain name).

Also mentioned in this video clip is remote support. This involves a technology to obtain third-party assistance for your own device without the need for an engineer to attend on-site. Financial institutions also use this to provide their support or helpdesk facilities. Please make sure to take the following measures when using this technology:

- Don't call any support or helpdesk numbers which are displayed to you in Google ads.
- Only establish connections with trustworthy people. You should be particularly cautious if it is not you initiating the connection.
- Make sure you are using a secure connection (with a lock symbol, the correct financial institution's name and the correct domain name).
- Don't grant full access to your system. The person helping you should only ever be able to view your screen passively.
- Take into account that everything shown on your screen can be seen and also recorded by the other side.
- Don't surf to any Internet pages which have nothing to do with the session – even if you are asked to do so.
- Make sure that the remote support connection is terminated after availing yourself of any help, to stop any further access to your device.