UniCredit Bank

PRINCIPLES OF SECURE COMMUNICATION AND DATA PROTECTION

Following these simple rules will allow you to securely control your accounts via direct banking products and minimise the risk that your personal data will be misused by unauthorised persons.

Login details, passwords, PINs

- Never disclose your security information (user ID, password, PIN, security code) to another person.
- Avoid using direct banking products in public (such as while using public transportation) and in monitored rooms (such as in the sight of security cameras).
- Be conscientious about your privacy and check that other people cannot observe your login data, especially when logging in.
- Do not work with direct banking using computers you cannot ensure do not contain malware (e.g. in public internet cafés).
- Do not leave your computer or mobile phone unattended; use keyboard locks and device access codes.

E-mail

- The bank never sends e-mails calling for disclosure of identification information, passwords, PINs, etc. Do not respond to such calls and please inform the Client line if you receive one.
- Open only trustworthy e-mails from known and expected senders. If an e-mail seems suspicious, it is risky to open it and to work with the attachments and links.

Internet

- You should only visit known and trustworthy websites on the Internet.
- Avoid downloading unknown files from the Internet to your computer. They can conceal dangerous programmes and viruses.
- If the login screen for your direct banking products seems suspicious in any way, do not log in. Instead, contact the Client line.
- Be especially cautious when using open wireless networks (use only trustworthy Wi-Fi connections).

Mobile applications

- You should only install applications from official application stores to your mobile phones – Google Play (Android), App Store (iOS)

Viruses

- Perform regular scans using an anti-virus program.
- You should update the program regularly. We recommend using up-to-date versions of anti-virus programs that also include malware detectors.
- We also recommend using a firewall on your computer.
- Even smartphones and tablets should be provided with anti-virus protection.

UniCredit Bank

Operating system, web browser

- Update your computer's operating systems with security patches or by using update packages issued by the manufacturer.
- You should also update your programs regularly; it is especially important to update your web browser and its plugins (e.g. Flash Player).
- For smartphones and tablets, we also recommend using the current versions of firmware officially offered by the manufacturer for the device.

You should check your account balances and transactions regularly – for example, by SMS messages or e-mails that are sent automatically and which include the appropriate content.

When suspected fraud, in case of fraud or security threat bank shall inform the Client in an appropriate manner, primarily after consultation with bank employee at the Client's branch and using contact information stated by Client when entering contractual relationship, respecting the security of shared information between the Bank and the Client.