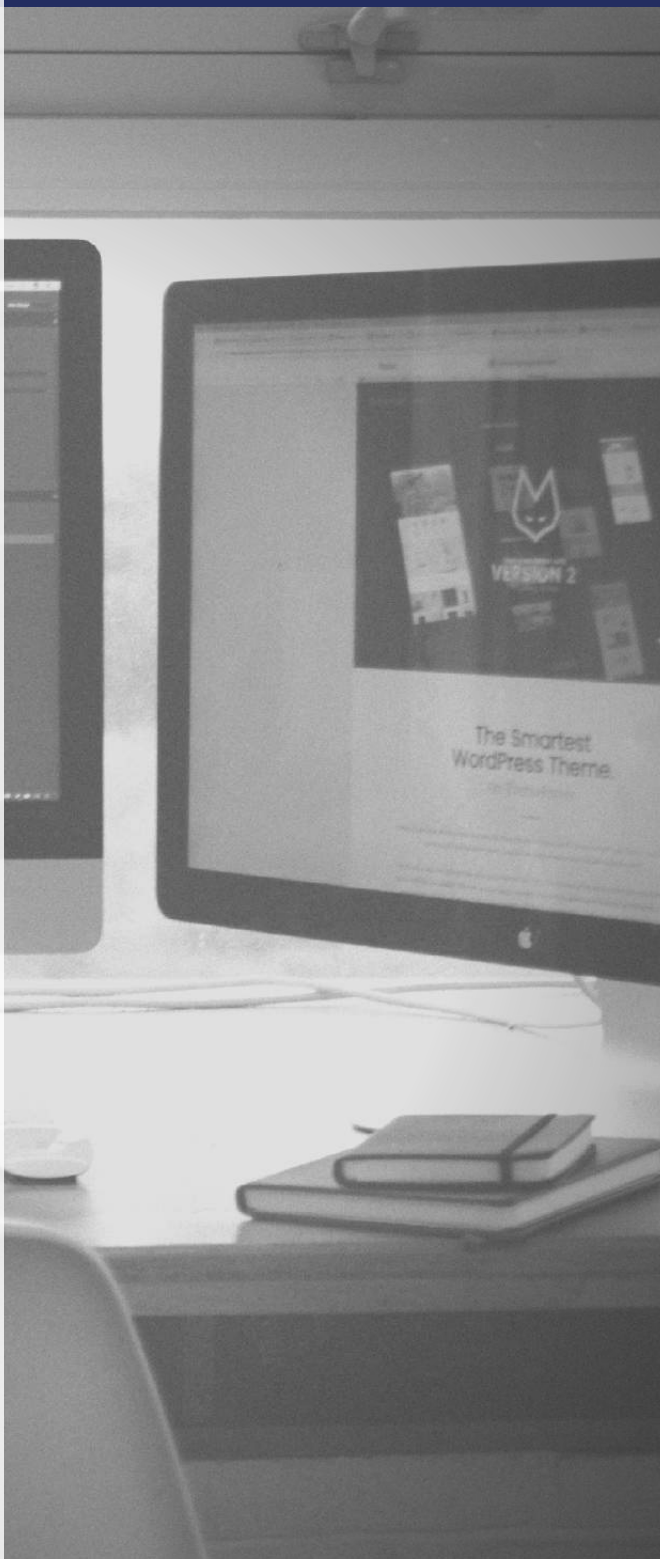
MIND SECURITY!

Eurasian Bank

Dear Customers!

Due to the increased danger of becoming a victim of cyber-criminals, you are kindly requested to follow these rules when using the remote banking service system (hereinafter - the RBS)



- Do not save the password for access to the RBS in the Internet browser and text files on the computer or other electronic media.
- Do not transfer your RBS password to the third party, including the Bank employees.
- Avoid connecting to the RBS website following the banner links or links contained in an e-mail.
- Make sure the SSL-connection to the RBS official website is secure.
- Avoid visiting other websites while using the system.
- Remember to end the session after you using the RBS.
- Avoid using the RBS in public Internet access points and guest workstations (for example, Internet cafes).
- Use password, pattern or biometric authentication to unlock mobile devices.
- If you lost the mobile device that you use to receive SMS-messages from the Bank, or your SIM-card suddenly went wrong, immediately call the Bank, and contact your mobile operator to block your SIM-card.
- Inform the Bank on unauthorized transactions in the RBS. For example, if you receive SMS-messages for an operation that have not been conducted. In such cases, you should immediately contact the Bank.
- Avoid to permanently work on your computer under the account with the administrative authority.
- Do not run programs obtained from unverified sources (programs received via e-mail or from the Internet may be of a particular danger).
- Do not visit suspicious websites or open doubtful emails.
- Use licensed software and timely install critical updates for the operating system.
- Update your antivirus signatures on a daily basis and regularly perform a full scan of your workstation for virus activity.
- Use additional security enhancement measures (firewalls, spyware scanners, etc.).
- Restrict the third party access to the workstation and other devices.