E-banking safety recommendations

As part of the constant care for its clients, Stopanska Banka AD – Skopje recommends at least the following security precaution measures every time you use banking online.

Select a strong password

- Strong passwords consist of at least eight characters and contain uppercase letters, lowercase letters and numbers. Select strong password when using E-banking service. The more complex the password is, the more difficult it is to guess. Do not use the E-banking service password for other web services such as webmail etc. Change passwords periodically, for instance every six months. Do not share with or tell your password to anyone.

Install security software

- There are many malicious software programs that monitor keystrokes and "phone home" periodically with the results of that monitoring. This type of virus is called a "key logger." To minimize the possibility of having your passwords stolen by a virus, install an Internet security program that provides complete protection from viruses and password theft. Select a program recommended by several trusted independent authorities. Security suites may include at least the following solutions: antivirus, malware protection, spyware protection, personal firewall, identity theft protection etc.

Do not click e-mail links

- Stopanska Banka AD – Skopje or its employees will never ask for your E-banking password. If you receive an e-mail asking to submit your E-banking user name and password, this is just a fraud attempt. Bank employees may however ask you to provide your user name, but not your password, in order to confirm your identity in case of a forgotten password, and only at your request.

Forms and ways of stealing banking information

- Zeus, also known as Zbot, WSNPOEM, NTOS and PRG, is the most common banking malware platform for online banking. This malware code infects your personal computer, and then steals your personal and banking information such as: payment card numbers, PIN codes, and expiry dates.
- **Important: Do not enter your personal and other financial data. Immediately call the Bank help desk for further steps.**
- Example of a possible malware for stealing your personal and banking information.

- **Important: When using E-banking service, Stopanska Banka AD - Skopje will never ask for your Payment card number, PIN code or any other information since:**
  - The usage of E-banking service is not dependant on your Payment card number and especially not on your PIN code known only by you.
  - The usage of E-banking service is established in a very strict process of getting a user name and password, which after the first logon is chosen and known only by you.

Usage of wireless internet access; public computers

- Avoid using the Bank E-banking service via free wireless hotspots commonly found at airports, shopping centers or restaurants, unless the mentioned internet access is not secured by Wi-Fi Protected Access (WPA) or WPA2. Other encryption techniques such as Wired Equivalent Privacy (WEP) can easily be decoded with appropriate software thereby disclosing your sensitive information.
- Do not use public computers or Internet-Café when using the Bank E-banking service. Use single computer or lap-top instead.

Monitor your accounts and history of transactions

- Watch closely banking accounts and history of transactions when using E-banking service. If you spot suspicious transactions not approved by you, even those with small amounts, please contact our 24-hour call center on (+389 2) 3100 109.

Logoff after completing your E-banking session

- If someone has physical access to your personal computer used for E-banking service, always logoff after completing your session. This step minimizes the risk of any physical access to the personal computer while the E-banking session is still active. The most secure and recommended way is to close the internet browser after ending the E-banking session.

Be cautious at all times

- Let safety remain your top priority when using the E-banking service. Every false sense of security can be a hacker's greatest asset.