1. **Protect your personal certificate and its private key**

   The personal certificate replaces your hand-written signature, so protect it against misuse by third parties. CSOB has selected one of the safest means of storing the certificates – a chip card from which the certificate cannot be taken out and without which it cannot be used. Therefore, protect your chip card as well and don't disclose its security PIN to anybody.

2. **Protect your PIN, don't use a simple PIN**

   The PIN you use to access the service or to use the chip card can be set to any number you like. Therefore, always select a PIN that is not simple and which cannot be guessed easily. On principle, avoid dates of birth, parts of phone numbers, consecutive digits, and the like. Please also use the longest possible length of the PIN.

   Do not write your PIN down anywhere. In particular it should never be on papers, in your computer, purse, diary or telephone device or on the chip card or payment card. Never allow your computer to remember the password. Do not communicate the PIN to anybody, not even to your family members. Destroy the original envelope with the PIN or keep it in a secure place (e.g., in a safe). Furthermore, the PIN shouldn't be stored in a place where your other personal documents are stored.

3. **Protect your mobile telephone**

   If you have authorisation codes sent by text messages please protect your mobile telephone, do not leave it unattended and do not lend it to other people. If you use a "smartphone" (a telephone with iOS, Android, Windows operating systems etc.), do not install unknown applications and download updates only from trustworthy sources.

4. **Check the payments that you authorise**

   Check the content of any SMS code message carefully. Make sure that account numbers in particular are correct. Do not confirm a payment that you have not entered yourself.

   What you should watch out for

   • If you are asked to enter an SMS code at a non-standard time when logging in or using electronic banking, or when you have not requested any transaction.

   • If the detailed transaction information sent in the SMS message with the authorisation code does not match the information shown on your computer or relates to a transaction that you did not enter.

   Read the whole SMS message with the authorisation code. Pay particular attention to the amount, the currency and the beneficiary account. SMS messages from the bank will always identify the transaction for which the SMS code was sent by the relevant transaction number. It must be the same as the number shown on the authorisation screen for the given transaction. This makes it easy for you to tell whether the SMS message was sent for log-in or for payment, and whether you yourself have entered the transaction. If the information in the SMS does not match the information on your computer or you suspect that you did not enter the transaction, do not enter the SMS code and contact the Electronic Banking Helpdesk.

5. **Protect your computer (incl. the operating system and the Internet browser)**

   Please regularly monitor updates issued by the manufacturers of your operating system. With their help then correct the errors and insufficiencies of these systems. For example, a procedure designed to protect the Microsoft Windows system is available at www.microsoft.com/cze/athome/security/protect/.

Under no circumstances allow your web browser to save log-in data.

6. Use a secure computer, protect your computer against viruses and spyware

When you use internet banking, please use only secure computers that are fully under your control, i.e. you can influence their security set-up. In no case do we recommend using computers unknown to you, e.g., computers in internet cafés or clubs.

Please use anti-virus and anti-spyware programs. Update them regularly to ensure they work as effectively as possible. Regularly monitor information about possible threats and new viruses on the Internet, e.g. on http://www.microsoft.com/cze/security .

7. Am I on my bank's website?

Please, check in your web browser whether the address of the log-in page starts with:

https://ib24.csob.sk/ - if using ČSOB Internetbanking 24, or
https://bb24.csob.sk/ - if using ČSOB BusinessBanking 24.

Check whether the website has a security lock icon. It means your website is encrypted. Double click on your "lock" and check it shows a valid certificate published by GlobalSign Extended Validation CA. CSOB now uses server certificates from GlobalSign to secure its the web pages for IB24/BB24 Services.

8. Install a firewall (security wall) to protect your computer

You should connect to the Internet through a firewall, which is a program or device that minimises the risk of unauthorised access to your computer from the Internet. The firewall only processes Internet queries permitted by you and filters out all other potentially dangerous data. It is possible to download a personal firewall free of charge, for example from www.kerio.com or www.zonealarm.com. Windows XP already contains a personal firewall, it is sufficient to switch it on.

9. Don't download unknown files from the Internet

Visit well-known and trustworthy Internet websites only. Avoid downloading unknown files from the Internet (especially those with the EXE extension) to your computer. Along with their original purpose, these files may also install dangerous programs on your computer.

10. Beware of untrustworthy e-mails

Don't open e-mail messages from unknown senders or messages with a suspicious name or suspicious contents. Never run the attachments to such messages and delete such messages without opening them.
Never react to an e-mail asking you to disclose your personal data, password or PIN. CSOB will never require you to provide your data in such a way!

11. Enhance your security by receiving SMS or e-mails

In the CSOB Info 24 service, you can opt to receive messages about all transactions made on your account or with your payment card.

Have you seen something suspicious? Contact us!

If you have any security-related suspicions, please call your bank on **0850 111 777** (from Slovakia) or **+421 2 5966 8213** or send e-mail to helpdeskEB@csob.sk.