



## Protect Yourself and Your Money!

We recommend to observe the following principles when using electronic banking services.

The same way you protect and guard your house, its locks and keys you should also protect your PIN and other identification elements.

### How to create a suitable PIN?

We recommend to select such PIN, which cannot be guessed easily (e.g. 12345) or derived (date of birth, part of phone number, first 6 digits of your birth number, etc.). Never write down your PIN. If you do so please, keep it on a safe place (e.g. safe box) but not in your valet, mobile phone, diary, PC or chip card.

Do not use a function of remembering your password and PIN in your computer. Never disclose your password and PIN to anybody.

If you wish to have an overview of your account movements, setup SMS or e-mail notification of your account or card transactions by CSOB Info 24.

Do you have security door on your apartment? Secure your PC!

Please, pay attention to your personal computer.

- **Monitor regular updates** issued by an operational system producer
- Install and update antivirus and anti-spyware software regularly
- Connect to internet using a firewall. Your personal firewall will block any unauthorized data transfer to and from your computer.

Professionals in this field can provide you detailed information on security of your computer.

Use a secure computer for your payment transactions only!

Do not use publicly shared computers, i.e. in internet café. They are not safe for electronic banking because they are not under your full control and you cannot influence their security settings. Safe computer is the one, which follows the rules above only.

If you work on your notebook, please pay attention to a trustworthy network connection. We do not recommend using free access networks at airports and squares because they may have insufficient security. Someone else can also access your computer.

Do you check who is behind your door before you open it? Use the same approach to unknown files and e-mails!

Please, visit known and trustworthy websites only. Avoid downloading unknown files from internet to your computer (especially files with EXE). These files can also install dangerous programs to your computer on the top of your original purpose.

Do not open e-mails from unknown senders or messages with suspicious names or content. Never open attachments of such messages and delete them without opening.

**Maintain your personal data safe. Our bank will never ask you for your complete identification data (PIN, password) by phone or e-mail.**



#### Am I on my bank's website?

- Please, check on your internet browser whether website address of your log starts with:  
<https://ib24.csob.sk/> - if using ČSOB Internetbanking 24 or  
<https://bb24.csob.sk/> - if using ČSOB BusinessBanking 24.
- Check whether a security lock icon is on your website. It means your website is encrypted.
- Double click on your "lock" and check certificate validity that it was published by GlobalSign Extended Validation CA. CSOB now uses server certificates of GlobalSign to secure its internet pages for IB24/BB24 Services.

#### Are you suspicious? Contact us!

If you have any security-related doubts, please call your bank at 0850 111 771 (from Slovakia) or +421 2 5966 8213 or send e-mail to [helpdeskEB@csob.sk](mailto:helpdeskEB@csob.sk).

