



GE Money
Bank

Rules for the Secure Use of Internet Banking

Contents

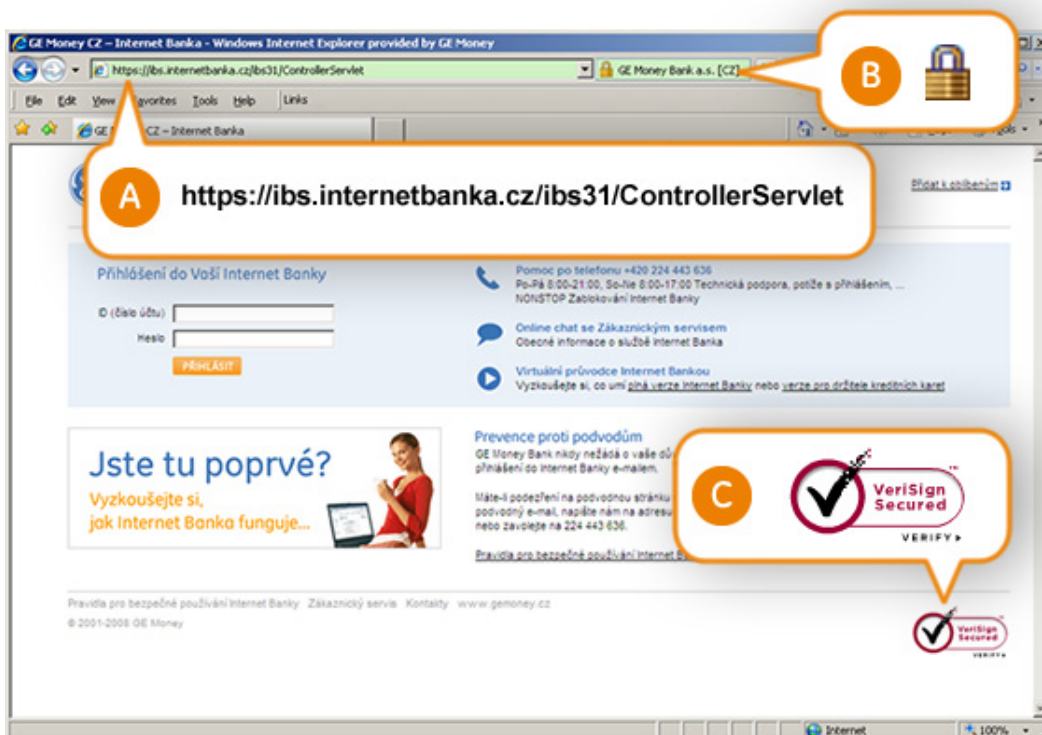
- Watch for Fraudulent E-mails and WWW Pages..... 3
- General Principles for the Secure Use of Internet Bank 5
 - Protect your Computer 5
 - Protect Your Passwords..... 5
 - Protect Your Security Certificates 6

Watch for Fraudulent E-mails and WWW Pages

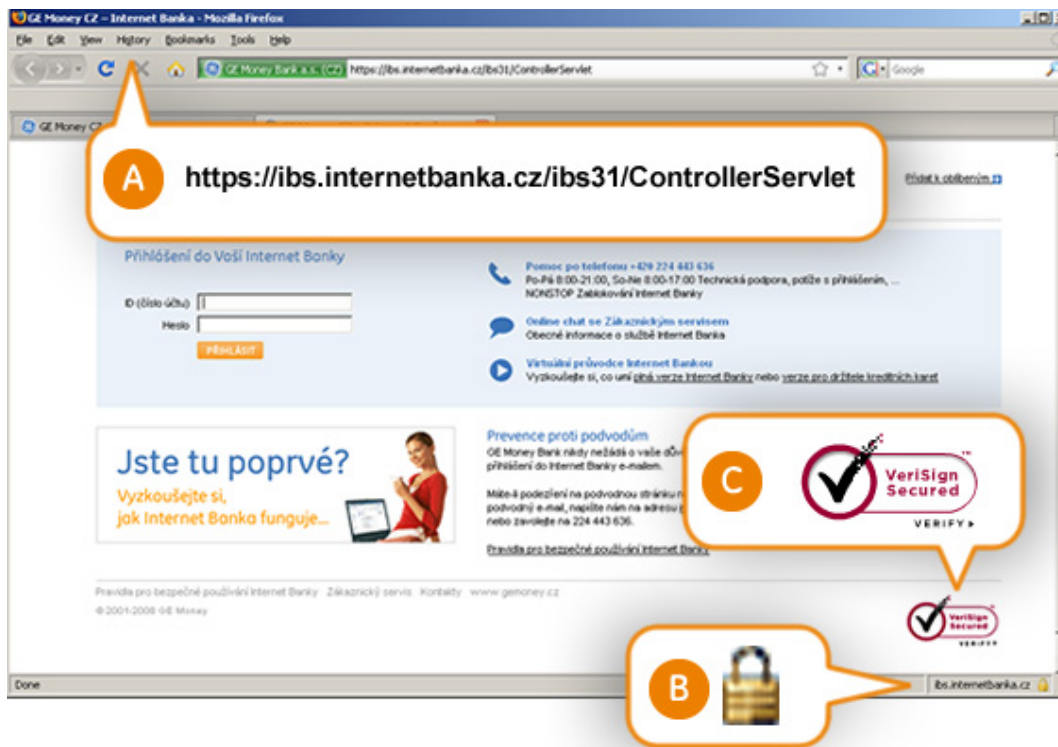
In order to jointly **prevent the abuse of your Internet Banking**, we request that you would thoroughly abide by the following rules:

- 1) Do not respond to e-mails that ask you to enter your personal data. **GE Money Bank never requests your confidential information, such as your Internet Banking log-in data, by e-mail.**
- 2) Make sure that you **log into Internet Banking at the right place**:
 - A) After opening the Internet Banking log-in page, check that the **following address is displayed in the command line** <https://ibs.internetbanka.cz/ibs31/ControllerServlet>. In new browser versions, the **command line background will turn green**.
 - B) Depending on the type and version of your Internet viewer, **an icon of a locked padlock** will be displayed in the top or bottom part. After clicking on the lock icon, information about the security certificate will be displayed.
 - C) The **VeriSign Secured logo** will be displayed in the bottom right-hand part of the screen. After clicking on the logo, a page with information will be displayed about the security certificate issued for the ibs.internetbanka.cz domain of GE Money Bank.

Preview of the log-in page in Internet Explorer, version 7



Preview of the log-in page in Mozilla Firefox, version 3.0



- 3) If you feel that the **log-in page behaves in an unusual manner**, for example, it **asks you for a password, mobile key, or signature certificate in an unusual place**, then do not fill in your log-in data. Contact GE Money Bank Customer Service at +420 224 443 636 and check that you are logging into Internet Banking in the right place.
- 4) If you are using **Internet Banking with a mobile key**, please pay attention to the entire text of the SMS message with the mobile key. For security reasons, **every SMS message** contains not only the mobile key, but also a **description of the transaction you are authorising**.
- 5) **Keep an overview of your money. Check your accounts** regularly. If you notice any unusual transactions, please contact us immediately.
- 6) If you **suspect a fraudulent page** or you have received a **fraudulent e-mail**, write to us at internetbanka@ge.com or call +420 224 443 636.

Further information about fraudulent e-mails (phishing) and www pages (pharming), and advice as to how to defend yourself, can be found, for example, on the pages of [Microsoft](#).

General Principles for the Secure Use of Internet Bank

In addition to the above, we recommend that you abide by the following principles of the secure use of Internet banking.

Protect your Computer

Keep your computer safe. Regularly **update the operating system** of your computer. Use a **current version** of an Internet **browser**. Install programs that will protect your computers, such as **antivirus programs, anti-spyware programs** and a firewall, **and update them regularly**.

Use a **filter for unsolicited electronic mail**, and do not open, but immediately delete, electronic mail and attachments received from unknown senders, as they can contain viruses and dangerous programs.

Avoid downloading and installing unknown files on your computer (especially those with an .exe suffix), as they can compromise the security of your computer.

If you are connecting from a place where several people have access to your computer, **do not leave your computer turned on unsupervised**. When leaving your computer, activate a password-protected screen saver or use CTRL+ALT+DEL to lock your computer.

Protect Your Passwords

Pay increased attention to maintaining the confidentiality of your passwords. **Do not tell your password to other persons**, even your family members. If you fear that you will not remember it, note it in such a way that only you have access to the note. Store the security envelope with your password in a secure place.

Change your password regularly, best every month. Change your password immediately if you have even the least suspicion that an unauthorised person knows your password.

Do not use simple passwords containing the names of your family members and dates of birth. Such passwords are easy to guess and abuse.

Do not permit passwords to be remembered in any of your computer settings. Never send your access password by electronic mail, even if someone asks it of you. **For security reasons, the**

bank must not request the sending of passwords by electronic mail. When entering your password, always make sure that you are entering it into an application operated by your bank.

For increased safety, you can have a branch activate the sending of information by SMS about logging-in to Internet Bank.

Protect Your Security Certificates

Treat your personal certificates cautiously, as well. If you have them saved on a flash disk or another medium, **never leave the medium in the mechanism** when not using Internet Bank, **and store it in a safe location**. If you have your certificates saved directly in your computer, place them such that no other persons have access to them.

If your signature certificate is **lost or destroyed**, and especially if you suspect that someone may have obtained a copy of your certificate, immediately **invalidate the certificate** in the Registration Authority application and generate a new certificate.

If you are connecting to Internet Banking from a publicly used computer (library, Internet café, school...) and if you use SSL and signature certificate as your security features, do not forget to remove those personal certificates from the computer before you leave, and close all connections with the banking server. In these cases, we recommend you use mobile key security.

If you suspect the abuse of your access rights, immediately contact GE Money Bank Customer Service at +420 224 443 636 and ask for your access to Internet Banking to be blocked.