DON'T GIVE IMPOSTORS A CHANCE

We never ask for your confidential data over the telephone or via e-mail on our own. This means that the bank itself does not approach the clients over the telephone or via electronic mail, or any other mail, to ask the clients to provide their confidential data to the bank.

We only require identification details from you when checking that you are authorised to carry out a transaction (for example, when you are logging in the telephone banking system we require the PIN and randomly generated characters from the password; similarly, the bank can, for example, request a further authorisation of a payment using a card. However, these are always cases when you make a transaction actively on your own).

This is the basic rule of secure communication, which will help you to detect that somebody may try to elicit important personal information from you, thereby gaining access to your bank account.

Fraudulent e-mail messages and websites can appear to be really very trustworthy, but they are so-called phishing – i.e. attempts at fishing for confidential data and subsequently abusing such data.

We would also like to draw your attention to another type of fraudulent transactions that may be directed at abusing your account for money laundering, which is an issue to which KB devotes a great attention. Some impostors can try to convince you, under the pretence of promising easy profit, to provide your bank account for precisely these purposes, without you being informed about these criminal intentions. The only way of avoiding such risk is not to respond to the e-mail messages that promise you a certain percentage of the profit if you accept money in your bank account, then collect the money in cash and send it, in cash again, to a specified address, usually to one of the republics of the former Soviet Union. Should you become involved in such activities you also become exposed to the risk of criminal prosecution and, understandably, potential abuse of your data.

WHAT SHOULD YOU BE CAUTIOUS ABOUT?

- E-mail messages and telephone calls whereby a purported employee of the bank tries to elicit data such as the PIN, password, certificate and where it is stored, etc. from you. For this, he/she can even give you very serious reasons such as your payment card stop-listing, bank account blocking, discrepancies in internal documentation, crediting of a considerable financial amount to your account, and similar. But the bank never acts like this and each such requirement is suspect! It may happen in some cases that your relationship manager will ring you up and enquire about the reason for a specific transaction in your account. However, he/she will never request you to disclose your PIN, password, certificate, etc.
- If you find in your electronic mailbox a message that you identify, on the basis of the above information, as a suspect message, never respond to it. Fraudulent e-mail messages may contain a link to a spurious website, at which you may be requested to provide your PIN, certificate and personal data. This website may appear to be quite authentic, but do not be misled. We never proceed in this way.
- Connect to KB's Internet banking mojebanka only using the address www.mojebanka.cz or www.kb.cz. Executing active transactions in the Mojebanka application is now also conditioned by additional authorization using the authorisation SMS code sent to your mobile phone.

SENDING NOTIFICATIONS OF THE APPROACHING END OF THE PERSONAL CERTIFICATE'S VALIDITY

KB's effort is to protect clients against potential abuse of personal and confidential information as much as possible, and therefore we have therefore also changed the mode of sending e-mail notifications of the approaching expiry of personal certificates.

These e-mail messages do not contain any active link to the Certification Guide application. This means that in these e-mail messages, the bank notifies you of the expiry of your certificate. If you want to continue working with it, please open, on you own, the www.mojebanka.cz site, from which you can safely run the Certification Guide application.

For working with certificates (for example, to pick up your certificate, extend the validity of your certificate, etc.) use only the Certification Guide application you can launch from the www.mojebanka.cz site. What steps should you take if you receive a suspect e-mail message or somebody has tried to elicit confidential information from you over the telephone?

First of all, never respond to such approaches, not even if the persons are threatening you with closing your account, cancelling your card, or a financial loss or penalty. In such cases immediately call KB's toll-free customer service line at 800 152 152.

IMPORTANT RULES FOR SAFE USE OF INTERNET BANKING

1. Protect your personal certificate

The personal certificate substitutes your own hand-written signature, and it is therefore the "access key" to your accounts and funds. Therefore protect your personal certificate against abuse by third parties. We recommend that you keep your personal certificate on a portable carrier (for example, a USB disk, a floppy, or a CD) and keep these carriers under control in a safe place. To enhance the safekeeping of your personal certificate, we offer the use of the Můjklíč smart card.

2. Do not use a simple password / PIN

A simple password or PIN can be deciphered and used more easily. Do not therefore use words or numbers that have anything in common with the names of your family members, their date of birth, telephone numbers, etc. For the password, we recommend selecting a combination of upper-case and lower-case letters, digits and special characters (a full stop, exclamation mark, question mark, etc.). The password should have at least eight characters. Select a different PIN for your Můjklíč smart card than your other PINs.

3. Protect your password / PIN

Do not write your password or PIN in any notepads, diaries, telephone sets, smart cards, etc. Do not authorise passwords storing in any setting of your computer. Stick to the rule that passwords should not be disclosed to anyone, not even family members!

4. Set sending of notifications

It is recommended to set sending of notifications (SMS or e-mail) informing you of all payments carried out from your account or payment card. Settings can be easily managed via the Mojebanka and Expresní linka Plus Internet banking.

5. Update your operating system on a regular basis

Regularly install update files that remove certain faults and security risks. Update files are available free of charge from the home pages of operating system manufacturers' websites. If you use the Windows operating system you can visit, for example, http://www.microsoft.com/cze/security/protect/, which provides a description of the basic steps to secure your system.

6. Use your own computer

For using direct banking services we recommend that you use only your home/company computer. Do not allow any unknown person to use your computer. Before leaving your computer, at all times use CTRL+ALT+DEL to lock the computer; with older operating systems activate the screen saver, which is protected by a password. For direct banking services we do not

recommend using a computer about which you know nothing (for example, a computer in an Internet cafe).

7. Use anti-virus software and anti-spyware

Always have anti-virus software installed on your computer; it improves protection against harmful programs - viruses. Similarly, it is appropriate to use anti-spyware (for example, Ad-aware, Spybot), which improves protection against the monitoring of your work on the computer by means of parasite programs. Update your anti-virus software and anti-spyware on a regular basis.

8. Access the Internet through a firewall

The so-called firewall serves to minimise the risk of unauthorised access to your computer when you connect to the Internet. It is a protective program or a technical device that processes only your queries sent to the Internet and filters away any other incoming (potentially dangerous) data. In Windows XP you can activate the firewall which is a part of the operating system. A personal firewall can be bought and downloaded from, for example, www.sunbelt-software.com, www.symantec.com or www.agnitum.com.

9. Do not download unknown files from the Internet

Visit only known and trustworthy sites on the web. Beware of downloading unknown files to your computer, which can also install dangerous programs together with serving their original purpose.

10. Open only trustworthy e-mail

Do not open e-mail messages from senders whom you do not know or messages that have a suspect title or content. Do not open the attachments to such e-mail messages and delete the message without opening it.

Do not disclose your personal data, passwords or PIN codes in an e-mail message. Komerční banka never requests such data.

Komerční banka also never sends unsolicited e-mail messages containing links to website addresses. If you receive an unsolicited e-mail message containing a link to Komerční banka's website, do not respond to the e-mail and do not click on the link.

CLIENT SPECIMEN SIGNATURES PROTECTION

Do not present your bank account specimen signature to any other person, neither in case the person proposes to provide you any service where your specimen signature is required.

A specimen signature different from your current signature is highly recommended. Moreover a specimen signature may include numeral or text information that only you know.

Security of authorisation of operations at the branch (e.g. cash withdrawal) may be significantly increased by using the optical key card (OPK).