ČESKÁ SPOŘITELNA

HOAX

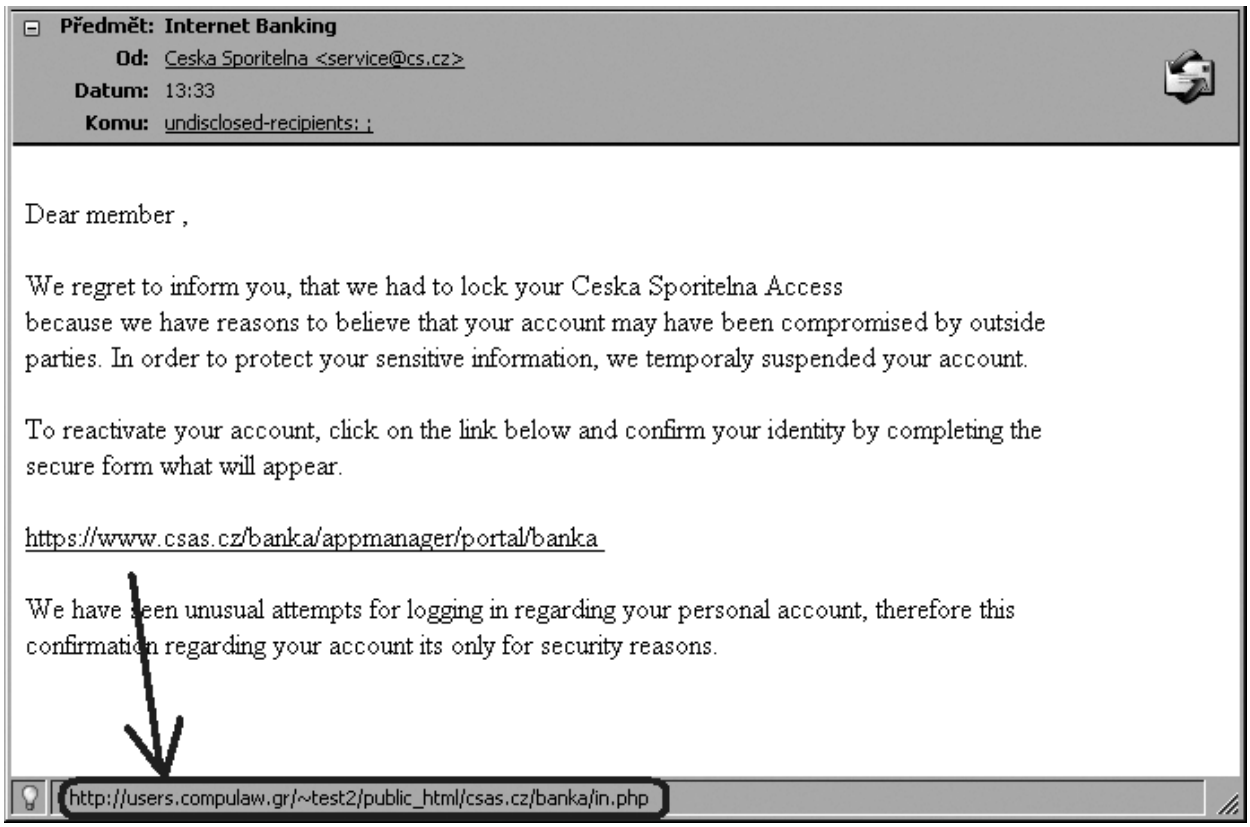
Do You Know the Basic Scams of Cyber Crime? Don't Get Taken In!

Internet security in context of money transfers and other financial transactions has become a widely discussed topic, not only in the Czech Republic. The open environment of the internet attracts offenders. Cyber crime is a serious crime – what are the basic types of this kind of fraud and how can you protect yourself?

What is phishing?
Phishing is a fraudulent e-mail sent out with the purpose of getting clients' confidential information. The authors of phishing want to obtain and consequently abuse data such as client's card numbers including information written on the reverse side of the card (protective code typed above the magnetic strip on the card known as CVV/VV code, which is only used for purchases from internet merchants). These perpetrators are also after access codes for the internet banking (clients number, password and other data).

Phishing – main features:
– Phishing creates the impression as if the message was sent from a bank official e-mail address. The sender's real address is hidden under a seemingly credible address.
– The fraudulent e-mail can look like a receipt of a payment order failure, call for security data update, notice of temporary blockage of the client's account or payment card, client satisfaction survey or even as an electronic newsletter for clients.
– The body of the e-mail contains a link which seemingly redirects to bank web pages. However, closer examination reveals that the e-mail refers to a fraudulent web page and prompts recipients of the e-mail to enter their confidential data.
– E-mails are often written in English, although versions written in good Czech without grammatical errors are on the increase.

Note: Czech clients, mainly clients of Ceska Sporitelna, have been confronted with phishing since the beginning of this year. Be cautious whenever you receive e-mails giving impression to have been sent from Ceska Sporitelna.



How will I know that I have received a fraudulent e-mail?
Phishing is easy to recognize: if you start to receive e-mails which were seemingly sent from a bank and contain links to web pages that require entering your access codes, you are a victim of phishing. The bank never sends out messages of that kind and has no reason to ask you for such information.

How will I be certain that I am on the web pages of the real internet banking?
If you do not encounter anything non-standard or suspicious, you are on the real web page.

– Never log on to the internet banking via links in e-mails!
– Always type in the address of the internet banking web pages to URL field of the browser on a newly opened internet page. The extra work will pay off by higher security.
– The address of the secured web page always starts with "https://" the letter "s" before the colon indicating secured communication of the internet browser with the server.
– No new additional data (besides those that you usually use) are required for the login to the internet banking. Similarly, no duplicate confirmation is needed.

Other techniques of cyber crime:
– Pharming – attack aiming to redirect a website traffic to another, bogus website. The user thus gets to a pre-created copy of a web page. The purpose of pharming is again to obtain and abuse the user?s confidential data.
– Trojan horse – keylogger is the typical example – the system tries to decipher the access information by capturing keystrokes entered by the user. The information is then forwarded to the authors of the keylogger.
– Malware – general term for intrusive software programmes. The attacked computers can serve for address collection, spam spreading, including phishing e-mails, and further distribution of malware.

All the fraudulent techniques elude security technologies and try to install themselves on a computer without the user's knowledge while the user is surfing the internet, downloading doubtful e-mail attachments or installing unverified programmes.

If you encounter any unusual or suspicious phenomena in your internet banking, do not enter any security information and terminate the application. Contact the client centre of your bank.

Note: Ceska Sporitelna monitoring has recently detected a new type of Trojan horse aiming at getting access codes to the internet banking from clients of several banks. Thanks to quick detection of the fraud attempt, no clients should be affected.

Who are cyber criminals?
Cyber criminals are individuals or, more often, group of people who carry out a whole range of activities aiming to enrich themselves or to cause general damage. Cyber crime involves sending out spam, distributing malware, infiltrating and consequently abusing insufficiently secured web servers. Spam with different contents including viruses and Trojan horses can infiltrate computers of current users, self-activate and cause harm. To fight against cyber crime is like to try to "grasp wind" – the internet knows no frontiers and cyber criminals thus recruit from different parts of the world – mostly from countries of the former USSR, China or from the American continent.

How can I protect myself against cyber criminals?
Mind these security rules:

– Update the operational system in your computer. If correctly installed, the majority of operational systems can regularly control, download and install the updates.
– Use a good antivirus program and update it regularly.
– Install an anti-spyware programme.
– Carefully protect your access codes and payment card data.
– Do not use publicly accessible computers placed in internet cafes when you access your internet banking.
– If you did give your security data away, contact your bank immediately.
– Purchase an electronic certificate on a chip card for maximum security. The investment of approx. CZK 1,500 in a higher type of security for your account is low compared to safety-lock for your flat or car.

Furthermore, the credibility of the server which administers your e-mail address should be taken into consideration. The server has no connection either with the banking server which operates your internet banking or any other server of the bank. If your e-mail address is filled up with spam, the administrator of the e-mail server presumably does care about anti-spam and other filters update. In that case it is worth considering a possible change of the provider of your e-mail service.

Information available on the internet:

In Czech
http://www.csas.cz/phishing
http://www.hoax.cz/ (http://www.phishing.cz/)
http://www.spyware.cz/

In English
http://www.antiphishing.org/
http://en.wikipedia.org/wiki/Phishing
http://en.wikipedia.org/wiki/Pharming
http://www.castlecops.com/

Prague, March 19, 2008

Issued by Ceska Sporitelna in cooperation with www.hoax.cz