Erste Bank warns customers of phishing e-mails

05.08.2011

Internet fraudsters are currently attempting to lure bank customers into giving them their online banking access data by so-called phishing e-mails. In various e-mails with senders like “SparkAsse“ or “Erste“, customers are requested to enter TANs into fake entry screens or enter access data (IDs and passwords) into login pages on fake URLs.

Currently, there are e-mails in circulation that request recipients to confirm their e-mail address or other data claiming that otherwise their account will “expire“. The e-mail contains a link to a fake website on which the user is requested to reveal personal data such as IDs, passwords, e-mail addresses, TANs or TAC or TAC-SMS. The language the e-mails are written in is very poor German.

These are not requests from the bank. Erste Bank and Sparkassen will never request their customers to reveal their PIN or TAN codes or to verify their accounts by e-mail.

Erste Bank and Sparkassen would also like to point out that neither Erste Bank itself nor the savings banks, s IT Solutions or s ServiceCenter will ever ask their customers for access data via e-mail. All recipients of such e-mails are warned against following such links and are recommended to immediately delete the message.

How to protect yourself

- The **real login page** for netbanking starts with: **https://netbanking.sparkasse.at/....**
- Save the real link under **favorites** and never use another link to enter your data
- Read such **e-mails carefully** and if you suspect anything, immediately call 05 0100 – 50 200 and ask
- **Never click** on any **links** in such e-mails
- Never enter TAC-SMS, TAN, ID numbers or passwords if **requested** to do so **by e-mail**
- Before entering sensitive data, check the **security certificate** on the website as well
- **Check** if the recipient account is correct in the TAC-SMS
- Use the latest software and **virus protection programs** on your PC

Secure Internet pages like the netbanking page of Erste Bank and Sparkassen are identified by the letters "**https**“ in the address line of the website and by the lock or key symbol in the Internet browser. Moreover, on the netbanking site, in most browsers the address line has a green background or a certificate symbol with a green background.

The ID number, the self-defined password and the TAC-SMS sent via SMS upon request guarantees the highest level of security. As the TAC-SMS is only valid for the current netbanking session for a limited time and exclusively for the transaction for which it was requested, its later use by attackers is not possible.

Example of a fake e-mail [pdf; 9.2 KB]