Erste Bank und Sparkassen Caution Customers Against Internet Fraudsters

Phishing emails increasingly circulating at present

Bank never asks for customer data via email

Customer PC: Beware Trojans

Currently so-called **phishing emails** are increasingly circulating. Toward the e-mail recipient they pretend to be messages from his bank. In most cases they contain links to fake login pages, which then ask under false pretenses for confidential customer data. “One should either forward such e-mails to the netbanking help desk or immediately delete them, and never enter any data”, says Günter Lazel, netbanking expert at Erste Bank. Erste Bank und Sparkassen never request any customer data, passwords, credit card numbers or other information from their customers. Under false pretenses such as e.g. “your account is expiring”, “please confirm your account” or “account activation update”, fraudsters currently try to elicit data from users.

The goal is to get hold of the login data and the TAN, respectively TAC codes of customers, in order to trigger a transfer in the background - most of the time to an account abroad.

In some cases there are also fraudulent phone calls after the data have been relinquished. In these cases the fraudsters pretend to be bank advisors and attempt to get hold of TAN or TAC codes. In these instances the rule applies as well: Be cautious, and never disclose any data over the telephone.

Trojans by contrast are infections of a customer's PC or smart phone. The malware (Trojan) installs itself in most cases on the computers of users without them being aware of it. One can be infected with Trojans while surfing various internet sites, which then download data from one's own computer in the background and spy out passwords. Such Trojans may also lead users to fake netbanking login pages. When trying to enter into netbanking, one is asked to enter one's netbanking login data under false pretenses such as “new products and security features” or similar prompts. “We recommend to regularly perform virus scans, switch on one's firewall and always implement all security updates”, explains Lazel.

The user number, the self-selected password and the TAC code transmitted by SMS guarantee the highest possible security. The TAC-SMS is only valid within the current netbanking session for a limited time period and solely for the specific transaction it has been requested for. With that further use by attackers is ruled out. However, if one receives a TAC-SMS in spite of the fact that one hasn't requested one, caution should be exercised. That happens if one hands over login data to third parties. With that orders can be entered and the transmission of a TAC-SMS can be triggered.

Don't forget the fact that smart phones are small computers. Especially the Android operating system is a popular target of attacks. All customers of Erste Bank und Sparkassen can obtain virus protection software for Android smart phones at a discount here: http://ebspk.ikarus.at/

How one protects oneself against....

Phishing Emails	**Trojans**
Be careful with emails from unknown senders and never click on any links they may contain	Regularly perform security updates for your operating system, switch on the firewall and install up-to-date anti-virus software on your PC and smart phone

Banks never ask their customers by email to reveal personal data such as e.g. passwords, TAN or TAC codes, credit card numbers, cell phone data or the creation dates of the TAN list, nor do they request updating of customer data.

If in doubt, always contact the help desk (05 0100 – 50 200), or delete the email without downloading any attachments or clicking on links

Make use of TAC-SMS and always check the TAC-SMS text (account number of payee and amount to be transferred) prior to approving a transaction

Make sure that the correct netbanking address is displayed in your browser's address bar, which is always SSL encrypted (lock icon) and begins as follows: https://netbanking.sparkasse.at/