www.netbanking.at

The netbanking system of Erste Bank and Sparkassen has developed into a veritable sales channel in recent years. It offers clients a variety of valuable functions and services at any time of the day and from any computer linked to the Internet.

The rising popularity of this sales channel is also revealed by the steadily increasing number of users. One in every five private clients with a bank account makes regular use of the netbanking service. One in every three manual transfers is no longer submitted in a branch but sent through the online system. By the end of 2005 the number of Erste Bank clients with access to netbanking had risen to 166,000, with 86,000 actually using the system in December 2005.

Throughout 2005 as a whole, the clients of Erste Bank made a total of 3.4 million transfers and submitted 20 million information queries through netbanking. On average, netbanking clients access the system nine times every month.

The entire Sparkassen Group comprised 549,000 netbanking clients and 285,000 active users in December 2005 (which constitutes growth from December 2004 when there were 240,000 active netbanking users), hence one in every six private clients with a bank account uses the netbanking service regularly. In the course of 2005 a total of 11.5 million transfers and 62.4 million information queries were submitted through netbanking (inquiries on account balances, credit card transactions, etc.). Netbanking clients in the Sparkassen Group also access the online system an average of 9 times a month.

In order to make the Internet presence of Erste Bank and Sparkassen even more customer friendly and to expand the range of services for clients, the online portal has been redesigned. One of the goals was to orientate prospective customers from the Internet into the branches. A further objective was to raise the number of products sold and managed via the Internet. This gateway to banking services was designed after the completion of comprehensive customer surveys and in accordance with the needs and requirements of clients. Particular attention was paid to ensuring that the range of products on offer and the key services were presented clearly and understandably, as well as expanding and simplifying the opportunities for using products online.

In addition to enhancing the customer friendliness of the portal, with online crime rising day by day Erste Bank and Sparkassen also focused on security issues as a priority.

Besides the now common security standards in netbanking such as safeguarding content by means of SSL (Secure Socket Layer) the application of additional encryption using cryptographic algorithms as well as further specific security measures, action was also taken to counter threats currently roaming around the Internet.

In May 2005 the transaction authentication numbers (TAN) were optimised. In order to prevent the direct use of a – theoretically – intercepted TAN, each and every transaction must be approved by a given TAN (which is no longer a number chosen freely from a list). The system recognises all of the TANs still available and for approving instructions always asks for a – randomly chosen – TAN, which is only valid for the given transaction.

As an alternative to this procedure, since May 2005 Erste Bank and Sparkassen have also offered the use of transaction codes (TAC) sent in TAC keys by text message.

The user number, the password and the reusable transaction code chosen freely by the client coupled with the TAC key sent via text message to the client's mobile phone guarantee the highest security. Since the TAC key is only valid within the current netbanking session and only for a limited time, it is impossible for it to be used subsequently by any unauthorised parties.

However, in order to boost security on and to prevent identity theft through the Internet, it is also necessary for users to sharpen their awareness of online security. The use of the netbanking system is put at risk primarily by end-user equipment being unprotected or if people act carelessly and thoughtlessly with regard to their access codes.

But the Sparkassen Group also offers information and tips in respect of security on the netbanking portal.

Erste Bank recommends the following to its clients with a view to enhancing their own security and protecting

themselves against such attacks:

- Be very careful with emails sent by persons unknown to you
- For your online banking only use the official netbanking site: www.netbanking.at
- Save this address in your browser as one of your bookmarks or write the address in every time.
- **Do not ever reveal any confidential data (login information, passwords, account numbers, etc.) by email or over the telephone.**
- If you have a mobile telephone, then in netbanking under the menu point "My Settings" enter the transaction code sent in the TAC key by text message that is valid for the transaction (additional text message code to approve transactions).
- Let us know immediately (by telephone, email or in person) if you receive such an email.

Thanks to the enhanced security measures and the awareness of clients, so far all phishing attacks on the netbanking system of Erste Bank have been unsuccessful.

Nevertheless, if a client does reveal confidential account information and passwords to an unauthorised third party by email, although this admittedly will enable access to account information it is still impossible to approve any transactions without having the additional codes.

We would also like to point out that there are repeated attempts made to recruit clients as "financial agents" or "finance managers". On Internet sites and by email dubious individuals contact account holders with the purpose of having them carry out a certain activity. This involves the account holders accepting sums of money from third parties on their own account that are derived from criminal activities, before forwarding the money on immediately after deducting a certain commission. Therefore such "financial agents" merely serve the purpose of conveying illegal money swiftly to third parties and covering the route of the transfer, which under these circumstances means they are also committing an offence.