RECOMMENDATIONS CONCERNING INTERNET BANKING SECURITY

By observing the recommendations, Internet users can help to make Internet Banking more secure.

SYSTEM SECURITY

1. Use trustworthy computers
   Ensure that only people you trust have the use or management of the computer system. Never carry out banking transactions using"untrustworthy" computers.
2. Use security optimised operating systems and browsers
   Only use computer systems that have been properly looked after and maintained. At the very least, the operating system should be regularly supplied with the latest developments in security software. Naturally the same applies in respect of your browser. You must activate the automatic updates and the phishing filter in your Internet browser. You can obtain more detailed information on these matters from your software manager or supplier.
3. Use virus protection and firewalls
   Use an up to date virus protection program with regular automatic updates against spyware, viruses an Trojan horses, or activate a personal firewall to protect your computer system.

Security of behaviour

4. Confidentiality of your personal access and authorisation data
   Never pass on your personal access and authorisation data, such as your log in data and cash transfer authorisation data (TAN) to third parties, and only enter these numbers on the verified Internetbanking ing page of the bank where you have your account. These confidential details must never be included in emails, forms or unknown Internetbanking systems.
5. The Bank's Internetbanking address (URL) must be entered manually
   Never follow links from emails or from other Internet sites to what appears to be the Internetbanking Portal of the main bank. The use of Bookmarks and Favourites is also potentially risky, as these can be manipulated by hackers.
6. Verifying Internetbanking sites
   You should carefully read and write down the Internetbanking address of your bank, so that you immediately recognise it when you next log in. Ensure that the connection is secure and encrypted. Such connections can be recognised by the lock symbol and by the fact that "https://..." is displayed in the address bar of the browser. If you suspect that the connection may not be secure, you should also check whether the encryption is activated by means of a digital security certificate. All you need to do is click on the lock symbol on your browser. You can verify that the security certificate is genuine here. Detailed data can be found in the security information provided by your Internetbanking provider. If only "http://..." is displayed in the address bar, the site is definitely not a legitimate Internetbanking site of your bank.
7. Do not file your user password and TAN on your computer
   Keep your confidential bank data in a safe place. As data can be spied out on PCs, we would strongly discourage you from storing this information on your PC.

Be aware of possible dangers

8. Be careful if you receive what appears to be an Email from your bank
   As a matter of principle Austrian banks do not send emails asking customers to reveal confidential access and transaction information, including user name and password. This type of email always constitutes attempted fraud.
9. Not the information provided by your bank, and report any indidents to the bank hotline
   Note the security instructions of your main bank as provided on the corresponding website. If you suspect any case of fraud, do not reveal any data and report your suspicions to the relevant bank hotline. You should also store the number of your bank's hotline on your mobile phone. If any security-relevant incident occurs, your password should be changed as quickly as possible via a secure connection.
10. Check your account statements regularly
    Check your account statements regularly for any discrepancies.

Issued by the Banking and Insurance Section of the Austrian Chamber of Commerce, in consultation with the consumer protection section of the Austrian Federal Ministry of Social Affairs and Consumer Protection.

Last updated: June 2019