

# E-banking security recommendations

By observing these recommendations, Internet users can contribute to making e-banking more secure.

## SYSTEM SECURITY

### 1. USING SAFE COMPUTERS:

Make sure that the computer system is used or administered only by people you trust. Never conduct banking business on unsafe computers.

### 2. USE OF SECURITY-OPTIMISED OPERATING SYSTEMS AND BROWSERS:

Use only properly maintained and serviced computer systems - the operating system should be supplied with the latest update of security software at regular intervals. The same also applies to your browser, of course. Activate the automatic updates and the phishing filter in your web browser. For further details, contact your software service representative or supplier.

### 3. USE OF VIRUS PROTECTION AND FIREWALL:

Use an up-to-date virus protection programme with regular automatic updates against spyware, viruses, trojans or activate a personal firewall to protect your computer system.

## SAFE CONDUCT

### 4. CONFIDENTIALITY OF PIN AND TAN:

Never pass on your personal access and authorisation data, such as your Personal Identification Numbers (PIN) and Transaction Numbers (TAN) to third parties and enter them only on the verified online banking website of the bank you hold an account with. Never enter confidential information in e-mails, forms or unfamiliar online banking systems.

### 5. ALWAYS ENTER THE BANK'S ONLINE BANKING ADDRESS (URL) MANUALLY:

Never follow hyperlinks in e-mails or other websites to the (alleged) online banking portal of your bank. Even the use of bookmarks (favourites, bookmarks) is risky since they can be manipulated by hackers.

## **6. VERIFY THE ONLINE BANKING WEBSITE:**

Read your bank's online banking address carefully and jot it down, so you will recognise it the next time you log in. Make sure the connection is secure and encrypted. Do this by verifying whether you can see a lock symbol and the prefix "<https://...>" displayed in the browser address bar. If you suspect the connection to be insecure, then check also whether encryption is enabled by means of a digital security certificate. To do so, click the lock symbol on your browser, in order to verify the authenticity of the security certificate. For detailed information, read the security information of your online banking provider. If just the prefix "http://..." is displayed in the address bar, then this is definitely not a legitimate online banking webpage of your bank.

## **7. DO NOT STORE THE USER PIN AND TAN ON YOUR COMPUTER:**

Keep your confidential banking information in a safe place. Since the data on a PC can be spied out, we urgently advise you not to store them on your PC.

### **WATCH OUT FOR POSSIBLE HAZARDS**

## **8. WATCH OUT FOR PURPORTED E-MAILS FROM YOUR BANK:**

As a general rule, Austrian banks do not send out any e-mails asking their customers to disclose confidential access and transaction data. This includes user number, PIN and TAN. These e-mails are invariably fraudulent.

## **9. OBSERVE BANK INFORMATION AND REPORT INCIDENTS TO THE BANK HOTLINE:**

Observe the security advice provided to you on your bank's website. When there is reason to suspect fraud, do not disclose any data and report your suspicions to the responsible bank hotline immediately. You should store also your bank's hotline number in your mobile phone. If any security-relevant incidents occur, change your PIN as quickly as possible, using a secure connection.

## **10. CHECK YOUR ACCOUNT STATEMENTS ON A REGULAR BASIS:**

Check your account statements for unusual activities on a regular basis.

**Published by the Bank and Insurance Division of the Austrian Federal Economic Chamber in consultation with the Consumer Protection Office of the Federal Ministry for Social Affairs and Consumer Protection.**