

# Security in Kathrein eBanking

November 2021

Online banking applications are popular targets for fraudsters. In order to circumvent security measures, they try to obtain user data via deceptive e-mails or malware, for example, and thus gain access to online banking. Kathrein Privatbank therefore recommends that you always be attentive and observe the following security advice when dealing with online banking. Only use the original website of Kathrein Privatbank.



As a general rule, Kathrein Privatbank will never ask you to disclose confidential data or grant remote access to your eBanking by telephone or e-mail. As part of an advisory meeting supported by the CommuniKATE function, you can also carry out a screen sharing with your Kathrein account manager.

## Protect your personal data!


Please always be extremely careful with your access data (signatory number, IBAN, PIN, security code, mTAN, etc.). Keep these data's secret!


- Do not give your access data to unauthorized third parties under any circumstances.
- Do not keep this data freely accessible and choose a secure storage location for your data worthy of protection.
- Do not write down access data so that they do not fall into the "wrong" hands, i.e. do not take photos, copies, or scans of them.
- Never store PIN/security code on the computer, smartphone, or tablet as a disguised phone number. Apps sometimes have access to your contact details and could get hold of the data.
- Make sure that no one is watching you when you enter your access data.
- Never use other people's open WLAN hotspots or publicly accessible terminals for online banking.
- Do not choose passwords that are easy to guess and change them at regular intervals or immediately if you fear misuse.

## Recognize Phishing-attempts!

Phishing refers to a fraudulent method of obtaining confidential data by means of unsolicited fake e-mails, SMS, messages in social networks, telephone calls or forms on websites. You are tricked into entering your confidential data by various pretexts (e.g. account/card blocking, charging of (high) fees, etc.).

- Delete unsolicited messages (e-mails, SMS, etc.) when you receive them and, if in doubt, clarify their authenticity with your counsellor!
- Never follow any links or open any attachments contained therein!
- Do not under any circumstances reply to such messages!


 Kathrein Privatbank will NEVER ask you to disclose your access data or security/signature codes by e-mail, SMS or telephone! Always keep your access data secret!


 If in doubt, contact your personal advisor directly. Use the telephone number or Kathrein e-mail address of your customer advisor that you already know. Contact details contained directly in the Pishing e-mail could be forged.

### Beware of malware!

Malware, so-called Trojans, or viruses, ask you, for example, via a fake page to "update security certificates or programmes/apps", to test a "demo account", to carry out a "test transfer" or similar. **Do not follow such requests under any circumstances and inform your personal Kathrein advisor!**

#### For your own protection:

 Never install programmes/apps on your computer/smartphone without thinking about it, especially if this is recommended to you without being asked (e.g. request via SMS, QR code, telephone, etc.).

 Only obtain programmes/apps from trustworthy official sources. Especially when downloading apps for mobile devices, make sure that they are offered via official stores (Google, Apple, etc.) and check them in advance (e.g. read the ratings of other users before downloading).

Beware of unsolicited contact from third parties (e.g. supposed technicians from well-known IT companies) - especially if you are asked to grant access to your computer/smartphone.

### Safety tips

**Pay attention to the encryption and the security certificate!** Check that the security lock is closed in the browser. Check the active encryption of the page by clicking on the security lock. In the window "Website identification", the note "This connection with the server is encrypted." should be displayed using Internet Explorer as an example.

### Use of current browsers or operating systems

Make sure that your Internet browser or operating system are always kept up to date with the latest security standards. To do this, install the updates recommended by the manufacturer.

### Use of antivirus and firewall

Use an up-to-date anti-virus programme or activate a personal firewall to protect your PC, tablet, or smartphone.



#### **Logout at the end of the Online eBanking session.**

Always end your eBanking or eSecurities Trading session by clicking on "LOGOUT".

### Our Kathrein security standards for login and authorization

Access to your account/deposit via the Internet is only possible with a valid combination of your username and personal password. In addition, a secure, encrypted connection (SSL) is used when accessing your account/deposit online. Furthermore, a two-factor authentication ensures that no unauthorized person performs online services with the account of the legitimate user. For additional verification, a one-time security code is sent by SMS to the user's mobile phone.

Furthermore, transactions via the Internet are protected by an mTAN medium, which is intended to prevent fishing due to its random composition. You will receive this mTAN as an SMS to the mobile phone number you provided during registration. The mTAN is inseparably linked to the order you have entered and is only valid for 5 minutes. For your security, the SMS contains brief information about the transaction. Before confirming (signing), always check the data displayed in the SMS for consistency with the transaction data entered online.