HAUCK & AUFHÄUSER
PRIVATBANK SEIT 1796

Security Instructions for the Hauck & Aufhäuser Online Banking

The security of your bank account and your data is our highest priority. Therefore, we are constantly developing our security architecture further and also cooperate with external specialists and consultants.

In addition, you can do a lot yourself for the security of your Hauck & Aufhäuser online banking:

Keep your PC protected:

- It is recommended that you update your antivirus program daily and automate this process.
- Use a personal firewall that provides additional protection for your PC.
- Turn off the possibility of caching encrypted pages on the hard disk of your browser (f.e. Microsoft Edge or Google Chrome) and keep your operating system and the programs you use always up to date.
- Do not carry out online transactions if you suspect that your PC is infected by a Trojan or virus.
- Always be aware of anything unusual when using the personal area to detect possible manipulation by a Trojan.
- If possible, do not log in to online banking via a computer you do not know (e.g. in an Internet café).

Protect your login data:

- Keep your personalized security features secret and transmit them only via the online banking access channels provided separately by the bank.
- Keep your authentication tool (PIN and mobile device) safe from access by others.
- When entering the personalized security feature, make sure that other persons are not able to spy it out.
- Keep the login name, PIN and, if possible, the authentication tool separate from each other.
- Do not pass on the personalized security feature outside the online banking process, for example by e-mail.
- Change your PIN regularly using combinations of upper and lower case letters, special characters and numbers. Do not use combinations that are privately related.
- Never enter more than one TAN at a time.
- Always use the log-out button in the upper right-hand corner to leave online banking. Always delete the cache after leaving online banking, unless you are the only one working on your computer.

Important notices:

- We will never ask you to make a "test transfer" or a "return transfer".
- Neither will we ever ask you to install any security software in the context of the mobileTAN/SMS-TAN for your smartphone, not by SMS or telephone call.
- You will never be called by us and asked for your access number and full PIN.

Stand: 01.08.2020