



The most important tips for safe online banking

Only use devices you're familiar with and wireless networks you trust

- Don't use any unknown devices to do your online banking. This is the only way you can prevent your information from being recorded and misused by third parties
- Use hotspots (wireless networks open to the public) only to surf the internet and not for online banking. Criminals can easily use an unsecured network to access your smartphone, tablet or laptop and find out your account details

Be careful with your login information

- Don't share your login information with other persons
- Don't save your login information on your PC
- Change your PIN periodically

Protect your computer

- Use a firewall and an updated virus scanner.
- You need to update your software programs to ensure that your PC is always up to date

Make sure you log out

- After completing your banking transaction, log out of online banking by clicking the "Log Out" button

Don't open spam

- Delete unknown or suspicious e-mails without opening them (spam e-mails)
- VTB Direktbank will never ask for confidential information from you, e.g. your account number, PIN or a TAN, via e-mail, on the phone or via SMS. Also, we never send you e-mails containing a direct link to your VTB online banking login which prompt you to enter your personal login information

Pay attention to transaction activity in online banking

- Regularly check your bank statements
- If you notice suspicious activity, block access to your account immediately and notify our customer service

Make sure you're on the right web page

- Regularly check the internet address you're connected to. The address "https://www.vtb-direktbank.de/..." must always be displayed in your browser. If the address is different, you should assume that you're not connected to VTB Direktbank
- In online banking, the internet address must begin with "<https://...>" and have a security certificate