wirecard bank E-banking security notice

The following information will help you increase the security of your bank transactions on the Internet. Please observe this information when using the Internet and particularly when making use of eBanking.

Handle your access data carefully and with caution

Just like when conducting business at a conventional bank or an ATM, when performing e-banking transactions always make sure that third parties cannot observe you entering password and access data (PINs). This particularly applies to transaction numbers (TANs). Please also make sure that third parties do not have access to your TANs.

Do not save any access or transaction data on your device. Choose a secure password and change it at regular intervals.

Ensure that your data is transmitted encrypted

E-banking should always make use of an https protocol. You can tell that this is the case when the beginning of the address bar in your browser changes. http:// turns to https://.

Check the authenticity of the bank website

Make sure that you are actually on your bank‘s website. You can do this by reentering the URL of your bank manually every time you open the site. If you are asked to enter a TAN when logging in or before starting a payment transaction you are most likely on a fraudulent site!

Try to restrict your e-banking business to one device if possible

Particular caution should be paid when using publicly accessible devices. Always log out from each session and delete the cache of the specific device.

Monitor your bank account movements on a regular basis

Check your bank statements on a regular basis. If your transactions seem questionable, contact the Wirecard Bank Service department immediately.

Ignore phishing mails and never respond to messages of an unknown origin

Your bank will never ask you for confidential data such as access data, PIN or TAN via e-mail, telephone, fax or SMS, i.e. by asking you to return or state this data or to directly enter access data. If you do receive messages of this kind, never click on websites or links contained in these e-mails. Inform us – but do not follow the instructions given to you in the e-mail.

Wireless connections

Activate password protection and encryption for all your wireless connections and check/change them periodically.

Optimum security with Mobile TAN Plus Service

The Mobile TAN Plus Service ensures optimum security by processing the transfer of the TAN and online banking via different transmission paths. If an attacker infitrates a PC, they will not be able to carry out any transactions unless they also have access to the mobile phone at the same time. For this reason, we recommend using two different devices for receiving the TAN and online banking.

Make sure your device is secured

Ensure your personal device is safe through the installation and the update of the relevant Security Checks (e.g. Anti-Virus Programs and Firewalls).

Software download

Please, be careful with the risks associated with Software downloads through the Internet. Make sure the products as well as their sellers are original and trustworthy.

Version: 1.0.0 | Status 4.12.2015

Wirecard Bank AG Serviceteam | P.O. Box 31 05 44 | 04163 Leipzig, Germany
Phone +49 (0) 30 / 300 110 600* | Fax +49 (0) 30 / 300 110 650 | service@wirecardbank.com | **www.wirecardbank.com**
Executive Board: Alexander von Knoop, Burkhard Ley, Rainer Wexeler | Chairman of Supervisory Board: Wulf Matthias
HRB number: 161178 (Munich District Court) | VAT identification number: DE 207567674 | IBAN DE75 7004 0041 0512 4805 00 | BIC COBADEFF700
* You will be charged by your telephone company for a call in the German landline.