F. Van Lanschot Bankiers (Schweiz) AG
Mittelstrasse 10, CH-8008 Zurich
Quai de Mont Blanc, CH-8006 Geneva
Postfach 3078 CH-8034 Zurich
Tel. + 41 (0)43 377 11 11

Security in E-Banking

Login / Identification

The E-Banking system of the F. Van Lanschot Bankiers (Switzerland) Ltd. is using state of the art security- and login-technology.

Your data is secured through a three-way authentication mechanism;

1. Your personal E-banking contract number
2. Your own chosen password (you need to change the initial password upon your first login)
3. The CrontoSign mosaic as a third security element for the login as well as the transaction authorization

After signing the E-banking contract it will be processed by the bank. Once processing is completed you will receive the aforementioned legitimation data (E-Banking contract number, initial password and the CrontoSign activation code) through separate mail.

Connection

In order to login to E-banking, please always use our secure E-banking link https://ebanking.vanlanschot.ch. **Do not** open the website through a link from an email or any other unsecure link.

Password

Obviously, cybercrime is a big issue these days and therefore secure passwords become more and more important. Please find below a few suggestions for a secure password.

- Change the initial password immediately after receipt (at least 8 characters).
- You need to use upper and lower case characters, digits and special characters (e.g. $, #,¦ etc.). To enhance the security, use longer and variable passwords without spaces.
- Do not use easily ascertainable combinations such as 123456, asdfgh, birthdays etc.
- Do not use 3 consecutive characters or numbers like aaammm, 111222 etc.
- Do not note down or store the password in an unencrypted form.

Please note; The bank will never ask you for your password by email or telephone. Therefore, please never give out any such details to anyone.

F. Van Lanschot Bankiers (Schweiz) AG
Mittelstrasse 10, CH-8008 Zurich
Quai de Mont Blanc, CH-8006 Geneva
Postfach 3078 CH-8034 Zurich
Tel. + 41 (0)43 377 11 11

Protection against manipulation

Besides password security, a safe technical environment is also of utmost importance. To reduce the danger against manipulations, we recommend to;

- update the used computer software on a regular basis
- use an antivirus program and a firewall with the latest technology
- read warnings and messages shown by the antivirus program and/or the firewall and adhere to the suggested solutions
- always use the E-banking at the beginning of an internet session
- not open any other internet pages during your E-banking session
- always use the „logout" function to safely exit the E-banking
- delete the browser history and the cache at the end of each session
- check the pending orders for correctness (e.g. beneficiary bank, account number, amount etc.)
- contact your relationship manager if you experience unexpected error messages
- not install any programs of unreliable/unknown origin (e.g. games or utilities downloaded from the internet, received by mail or from other sources). Such files can contain viruses, worms or a Trojan horse that allows malicious usage of data and can take over control of your hard disk.

If you have any further questions, please contact your Relationship Manager.