



Guidelines for Secure Usage

1. Never disclose your online bank user ID, passwords for your online bank, or any banking information to anyone over the phone, on social networks or by email.
2. If you have received a message on your phone from your login device to enter your password, but you are not currently connected to the online bank, ignore it.
3. When creating your passwords do not use or include the information related to your personal information, including information about family members which can be known or easily accessed by third persons, such as birth dates, names, surnames or pet names of family members/friends or their fragments. Also, it should not consist of easily memorable and/or guessable combinations of numbers and letters. You should avoid using any frequently-used words, simple words, phrases, and patterns that are easy to guess, like "Qwerty", "abcd", "12345", words like "password".
4. Do not write down, email, text message or otherwise share or save codes and passwords used to unlock your computer or phone screen.
5. Protect the computer or mobile device you use to connect to online banks: Install trusted, legal antivirus software, update your software regularly and use the latest browser versions. Security vulnerabilities in operating systems and other software are often found, allowing scammers to gain unauthorized access to other people's computers and systems which leads to personal information leaks. Please note that you are responsible for safety of devices used to log in to the Account, therefore it is highly recommended not leave devices from which you log in unattended, in public places or otherwise easily accessible to third persons
6. Always double-check the full name of the website (<https://fincause.com/>) and the overall look of the website. If any other domain is used or the HTTPS protocol is not used, it is highly probable that the website is not real and logins to such website could lead to your data being stolen.
7. At least once a month check your payment transaction history and inform us in writing about any unauthorized or inappropriately executed payment transactions if you notice any.
8. If you lose your password, other means of identification, payment instrument or any of your means of identification become disclosed to third persons or if there may be a real risk of unauthorized access to your account you or your representative shall immediately change your password (if possible) and inform us immediately via writing.
As a financial institution we do request personal information, but only through safe and confidential means, and only the necessary amount for us to provide safe and stable

financial services. This is known as the Know-Your-Customer principle, and it is accepted and implemented in financial services worldwide.

The Know-Your-Customer principle is a mandatory procedure in accordance with the Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing.

This data is collected to identify our customers' payment habits and sources of revenue to be able to respond to irregular activities relating to payment transactions and prevent possible fraud. You can read more about the Know-Your-Customer principle and the data that is collected in this article published by The Bank of Lithuania (https://www.lb.lt/uploads/documents/files/Know_your_customer_2023.pdf)

Lastly if you have any doubts or suspicions about the authenticity of any correspondence you receive claiming to be from or linked to FinCause or its representatives, please contact us immediately by any of the following contacts:

By email: support@fincause.com

By phone: +37064121390