How to use the Paysera services safely?

The Paysera system is completely secure, however, the security of the account and data also depends on your actions performed on the internet. The recommendations below will help to ensure the security of your actions performed on the Paysera account and on the internet in general.

Account

You can log in to the Paysera system via the mobile app (by entering a password or logging in using biometric data) or via the desktop version.

Log in via the desktop version by taking the following steps:

1. Go to https://www.paysera.com click *LOGIN* and you will be directed to https://bank.paysera.com/en/login.
2. Select the identification method – email address or phone number. Enter the selected data.

3. Select the account login method:

- via the mobile app. When using it to log in, you will have to confirm the control code in the app (it must match the code displayed in the browser window). Open the Paysera app and slide a confirmation bar if the code displayed on the login screen matches the code on the app. Touch ID or Face ID are recommended to be used for app access identification in order to ensure higher security.
- by entering a password. After entering it, you will access your account and will be able to see your account information, but will not be able to use any functions. To fully manage your account, you will have to confirm the login: in the upper menu on the left, tap *Login confirmation* and select the method – via the mobile app or SMS. Please note that the SMS service includes additional charges.

#

#

Please note several very important security rules when logging in to the account via the desktop version:

- open a new browser window and enter the address https://www.paysera.x (only the following domains may be entered instead of x: **lt**, **com**, **lv**, **bg**, **ee**, **pl**, **es**, **de**, **ro**, **al**, **ge**). In the upper right corner, click Login and you will be directed to https://bank.paysera.com/en/login. Make sure that the connection is encrypted (the lock is visible, and the address starts with “https”, please make sure that the letter “s” is placed at the end – in some cases, it is visible only if the address bar is clicked), and for a secure connection, an electronic certificate is issued only to the Paysera company, as displayed in the picture.

The Paysera system is not accessible at other, even very similar, website addresses, e.g.: www.payssera.com, bank.paysera.anotherdomain.com, paysera.myf1ntech.com/paysera/login, etc.

If at these kinds of addresses, you reach a website that is very similar to the official Paysera website, it is very likely that you ended up in a criminal trap. In this case, do not enter any data and notify the Paysera Client Service Centre immediately.

- always log out from your account. Avoid logging in to your account on public computers or devices of other persons because they may contain malware stealing passwords or other data.
- we recommend checking the IP addresses from which your account was accessed at least once a month. You can do this by clicking Settings > Profile Settings > Login history. If you have a suspicion, check if there were any transactions or logins from a different IP. The system allows the client to set IP addresses on their account from which the login to the client account will be available: Settings > Profile Settings > Additional security measures. If you have a suspicion, please immediately contact the Client Service Centre.
- do not transfer account login credentials to anyone. If someone has offered you to open a Paysera account on their or another person’s behalf or perform financial actions, contact the Client Service Centre and you will be advised on the next steps.
- update your personal and contact details immediately if they change. In case of security incidents or to provide important information to you, Paysera employees may need to contact you instantly and/or properly identify you.
- newly registered clients in the Paysera system should pay attention to the KYC questionnaire. The picture on the right depicts how it looks in the Paysera mobile app.

Please note that Paysera employees who contact you will never ask you to disclose your login details or transaction confirmation codes or passwords. Paysera employees may request certain login data only if you **yourself call** the Client Service Centre and **only for personal identification**. If you suspect that you are not talking with a Paysera employee, ask them to call you later and contact the Paysera Client Service Centre.

#

Account password

The account password must be unique and consist of at least 8 characters, uppercase and lowercase letters, numbers, and special characters.

Please do not use your personal information or the information of your family members in the password, for example, the date of birth, names, or surnames of your family members or friends, names of pets, or numbers and letters that can easily be guessed.

Please try to memorise the password and do not keep it in your notebook, on your phone, or elsewhere. We suggest using password storage applications and keeping your password encrypted.

Do not use the same password in other systems because it may also be used to log in to your Paysera account. If you suspect that other persons know your password, change it immediately and check if there have been any unauthorised logins to the account and if there have been any actual or attempted payment transactions.

We recommend changing the password at least every 3–6 months.

Please note that **Paysera does not send any messages requesting to change the password**. Even if Paysera notified you about threats to your data or account, or informed you about the need to perform any actions, messages **will never contain a link** to a password changing page. Paysera also never **requires its clients to download** attached files, install software, or disclose login codes. After receiving such a message, please immediately inform the Client Service Centre.

#

Smart devices

Use only those smart devices that have been legally acquired and officially imported, whose operating system software has not been modified (hacked), and on which applications from sources other than Google Play and the App Store have not been installed.

When a smart device is not in use, it must be locked with a code, password, or by other means. The lock code of the device and the Paysera app PIN code should not match parts of your phone number, car number plates, birthdates, or other numbers relevant to you – all codes must be unique and Face ID or Touch ID should be used.

The pre-installed and other application software must be updated immediately after the release of updates is announced by the software manufacturer. The manufacturer’s updates are intended not only for eliminating malfunctions, but also to patch gaps in security, and this is one of the guarantors of the security of the operations performed with your device.

In all devices that you use to connect to the Paysera account, install antivirus software. We also recommend installing a firewall, especially on computers, as this would prevent logging in to the computer from the internet.

#

Other actions online

Be careful when providing your personal data online, make sure that you provide it on a reliable website.

Before shopping online, check the reputation of stores in buyer forums and on rating websites. A newly registered store name (domain), the absence of the company’s real name, registration number, and contact information may indicate the low reliability of the store. Please also note the website address – whether it begins with something other than the http**s**:// characters, and if the letter “s” is present.

When shopping online, payments by card are often suggested and card data is requested. Shop there, where special logos confirming the security of payments are available: 3D Secure, Verified by Visa, and Mastercard SecureCode.

Do not click on web links that are unknown or masked, e.g. shortened, do not disclose the true source, appear on social networks, or are sent by SMS or email. Do not open unknown documents, do not install software from unknown sources, and do not visit unsafe web pages.

#

#

Certified security

The security of the Paysera system is confirmed by the international standard of security technologies and processes PCI DSS (Payment Card Industry Data Security Standard). This security standard regulates requirements for companies accepting card payments and processing client data. The highest standard of level 1, intended for the secure performance of over 6 million card transactions annually, has been installed in the Paysera system.

#

In case of any suspicious situations: a suspicious message on behalf of Paysera, suspicious transactions, loss of login data or entry of data on a false website, etc., please contact the Paysera Client Service Centre immediately. We will always help you find a solution!