

Customer Security and Fraud Awareness

Our Approach to Security

When it comes to your financial information, your security is our top priority and when you access your e-money account, it is important that we know it is you. Here are some of the ways we do that:

Login details – we provide you online login details unique to you, to protect yourself we recommend you do not share them.

Account Verification Questions – If you contact our customer services team, we may ask you to confirm who you are by asking you a unique question in relation to the company your e-money account is connected to.

Email Whitelisting - We send unique one-time use links to your whitelisted email for added security when:

- Create your personal e-money account;
- Create your PIN;
- Activate and/or pair your card(s);

Providing Information – we will never ask you for your online password details or PIN number. We will always first send you an email if we are trying to contact you.

How to Report Fraud

If you notice something suspicious and believe it could be fraudulent, you should contact us as soon as you become aware of it using the phone number +45 7876 8435 / +44 0330 808 1006, email fraud@pleo.io/ support@pleo.io

Reporting Fraud: fraud@pleo.io / support@pleo.io

Lost or Stolen Cards:

1. Log in to your App or Website account
2. Click **Cards**
3. Select the Card (**Virtual** or **Plastic**) which has been Lost or Stolen
4. Click **Disable card**
5. Click **Card has been Lost** or **Card has been Stolen**

6. Contact fraud@pleo.io to report unknown transactions

Suspicious Emails: fraud@pleo.io / support@pleo.io

How to Protect Yourself from Fraud

Help to keep yourself safe from fraudsters by following the tips below. Remember, if you are ever unsure, don't act on any suspicious requests, but instead contact support@pleo.io. A genuine company will never rush you to take action.

Always make sure your email address registered with us is up to date, and if you are an admin, that your mobile telephone number is up to date as well. We will use these to contact you if we notice unusual activity on your e-money account.

Some Tips for Using Your E-money Account and Prepaid Card Safely

When accessing your e-money account online:

- o Use an antivirus software and firewall.
- o Make sure you keep your computer and browser up to date.
- o Use secure networks.
- o Use strong passwords.
- o Don't share any passwords including whitelisting links sent to you.

When using a mobile application

- o Only install apps from recognised app stores.
- o Consider the app ratings and reviews.
- o Be aware of what permissions you are granting.
- o Treat your phone as your wallet.

When shopping online or in a store

- o When using an online retailer for the first time, do some research to make sure that they are genuine.
- o Do not reply to unsolicited emails from companies you don't recognise.
- o Before entering your prepaid card details, make sure the link is secure. There should be a padlock symbol in the browser frame window which appears when you login or register, if this appears on the page rather than the browser it may indicate a fraudulent website. The web address should begin with <https://>, the 's' stands for secure.
- o Always log out of website after use. Simply closing your browser is not enough to ensure your data is safe.
- o Keep your PIN safe and do not share it.

- o Keep your login details to your e-money account safe and do not share it.
- o Keep your card safe and do not share it. Your card is strictly personal and card sharing or reassigning is not permitted.
- o When entering your PIN, check for people around you and hide your PIN number.
- o Always check your statements and enable mobile app notifications for better awareness of activity on your account.

Remember, if you decide to donate, resell or recycle an old mobile phone, computer, laptop or tablet, make sure you fully remove all data and apps first as otherwise these may be accessed by whoever your device is passed to.
