Customer Security and Fraud Awareness Website Communication

18.11.2022

Contents

1. 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. Pleo will never ask you to disclose your personal details or OTPs. One Time Passwords are for you and should not be shared under any circumstances.

→ 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:
1. Create your personal e-money account;
2. Create your PIN;
3. 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.

→ Pleo calls

If you get a call from Pleo and it does not feel right, hang up. Instead call us back on the number on our webpage.

2. 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:

→ By phone

+45 7876 8435 / +44 0330 808 1006

→ By email

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

Please contact: fraud@pleo.io / support@pleo.io

3. 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

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

When using a mobile application

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

When shopping online or in a store

- When using an online retailer for the first time, do some research to make sure that they are genuine.
- Do not reply to unsolicited emails from companies you don't recognise.
- 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.

- Always log out of the website after use. Simply closing your browser is not enough to ensure your data is safe.
- Keep your PIN safe and do not share it.
- Keep your login details to your e-money account safe and do not share it.
- Keep your card safe and do not share it. Your card is strictly personal and card sharing or reassigning is not permitted.
- When entering your PIN, check for people around you and hide your PIN number.
- 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.

4. How to protect your iWallet from fraud

→ Apple:

If you lose your iPhone, iPad or iPod touch or think it may have been stolen, use Find My and protect your data.

- Look for your device on a map
  To find your device, sign in to iCloud.com/find. Or use the Find My app on another Apple device that you own. If your iPhone, iPad or iPod touch doesn't appear in the list of devices, then Find My hasn't been turned on. But you can still protect your account if Find My hasn't been turned on.
- Mark as Lost
  When you mark your device as lost, it will be locked remotely with a passcode, keeping your information secure. This will also disable Apple Pay on the missing device. And you can display a custom message with your contact information on the missing device. Mark your device as lost.
- Report your missing device to the police
  The police might request the serial number of your device. Find the serial number.
- File a Theft and Loss claim
  If your missing iPhone is covered by AppleCare+ with Theft and Loss, file a claim for an iPhone replacement. File a claim.
- Erase your device remotely
  If you erase a device that had iOS 15, iPadOS 15 or later installed, you can still use

Find My to locate the device or play a sound on it. Otherwise, you won't be able to locate the device or play a sound after you've erased it. If you have AppleCare+ with Theft and Loss, do not erase your iPhone until your claim has been approved. Erase your device.

- Contact your wireless network provider
  If the missing device is an iPhone or iPad with mobile data, report your missing device to your wireless network provider. Ask the network provider to disable your account to prevent calls, texts and data use. And if your device is covered under your wireless network provider plan, file a claim.
- Remove your missing device from your account
  If you have AppleCare+ with Theft and Loss, do not remove your lost iPhone from your account until your claim has been approved. Go to appleid.apple.com to remove the missing device from your list of trusted devices.

→ Google:

If your phone, tablet, or laptop is lost or stolen, follow these steps to help secure your device. If you can't get the deviceback, taking a few steps right away can help protect your information.

- Secure your lost phone, tablet, or Chromebook
  You can try some remote actions, like ringing, locking, orsigning out on your device. Lost a Windows, Mac, or Linux computer? Computers aren't listed under "Find yourphone." Move on to changing your Google Account password.

  1. Open a browser, like Chrome Chrome. If you're using someone else's device, use private browsing mode.
  2. Open your Google Account.
  3. In the "Security" section, find "Your devices". Select Manage devices.
  4. Select the lost phone, tablet, or Chromebook. You'll see the last time the device was used, and the lastcity it was in.
  5. Next to "Account Access," select Sign out. Follow the on-screen instructions to remove access to yourGoogle Account and connected apps on your device. If you find your device, you can sign in to yourGoogle Account again. If you're trying to find a lost phone or tablet, you can also select Find a lost device.

  Follow the onscreen directions for more ways to find or secure your device. If you're using someone else's device, when you're done, sign out by closing private browsing mode.

- Change your Google Account password
  Your Google Account password is the same password you use for Chrome and other Google products, like Gmail and YouTube. Learn how to create a strong password.

  1. Open your Google Account. You might need to sign in.
  2. In the "Security" section, select Signing into Google.
  3. Choose Password. You might need to sign in again.

4. Enter your new password, then select Change Password.
5. Change password

- Change your saved passwords
  If someone else has your lost device, consider changing the passwords that were saved to your device or Google Account.

  1. Open passwords.google.com.
  2. Sign in to your Google Account.
  3. Look at the "Saved passwords" list.
  4. This list only includes passwords saved to your Account, not your lost device.
  5. For each password you want to change, open the app or go to the site.
  6. Change your password.

*Monitor your accounts for fraud. Keep an eye on your credit card statements, and report any fraudulent purchases to your credit card company.

5. Some tips on how to prevent fraud via ApplePay/ GooglePay

Public Wi-Fi networks are surely a convenient way to enjoy free browsing (especially when you're abroad and don't want to pay for data roaming). Still, they are often unsecured or use unsafe passwords like "12345678" or "admin admin".

If you happen to add your card information to Apple Pay while using an unsecured Wi-Fi network, a hacker can easily intercept it so as to avoid changing anything in your Apple Pay profile when you're away from home. If you need to make urgent changes, consider using a Virtual Private Network (VPN). Keep your usage of public networks to a minimum

You may receive fake emails with statements claiming you've made a payment or are about to receive some funds as a grant, casino, or lottery win. Worried, you will click the link that should send you to the Apple Pay website for a refund or prize money. Use common sense. Watch out for "fishy" emails (pun intended) and ignore them

The way you can get scammed with Apple Pay is the same as you could get scammed while using any other payment system. Scammers make you transfer your money via Apple Pay to appear as if it was your own choice. Never transfer money to unknown websites, always double-check payments before completion, block strangers requesting money.

6. Scams

Since the start of the pandemic, we've seen a spike in scams where fraudsters try to convince

you to provide your account login details. Some of the most popular online scams to be aware of include:

→ Phishing

Phishing is a method of email attack in which the scammer sends out an email pretending to be Pleo in order to steal your passwords or sensitive information. They can then take full control of your computer.

Scammers will copy the logos, the style of genuine messages and ask you to take action, usually urgently. Let's say you receive an email from Pleo informing you that your account will be disabled within 24 hours due to an error with your account. It contains a link asking you to click on it to update your details. If an email address looks odd and you are asked urgently to click the provided link, it is probably a phishing attempt. Do not click on the link and report the email as a scam.

Here are some of the ways to protect yourself:

- Be skeptical and vigilant – does it look like a real Pleo email? You should only receive emails from addresses ending in: **pleo.io**, **hello.pleo.io** or **info.pleo.io**
- Check if the message contains a mismatched URL or a URL containing a misleading domain name
- Check for typos – poor spelling and grammar are often the first giveaways of a scam email
- If you're still unsure about the legitimacy of a link, ask the opinion of a friend or family member, or speak with our support team in the app.

→ Vishing

The term vishing comes from 'voice' and 'phishing'.

Let's imagine that you receive a phone call from someone who claims to be an employee of Pleo and collaborates with the Fraud department. The caller tells you about some potential fraud or suspicious activity on your Pleo card and you must urgently confirm your card or login details. This is information that Pleo would never ask for. Once this information is provided, the attacker can impersonate you and use the information collected for their personal benefit.

This is known as vishing. The 'visher' will use all kinds of techniques to convince you to provide your personal information – they can even change the phone numbers, email addresses and company names that appear on your device, so you think you're being contacted by a genuine company. This is called spoofing.

Here are the ways to keep yourself safe:

- Do not share information over the phone: Pleo will never ask you to disclose your personal login details or One Time Passwords (OTPs) over the phone. OTPs should not be shared under any circumstances.
- Keep your personal data safe. Never let anyone see your passwords or share images

containing phone number, card details or any other personal information on your social media.

- Don’t answer phone calls from unknown numbers. If you suspect you are being called by Pleo, please phone us back.
- If you’re still unsure about the legitimacy of a call, ask the opinion of a friend or family member, or speak with our support team in the app.

→ Smishing

This type of scam comes in the form of a text message. Often, it will contain a fraudulent link that takes victims to a form that is used to steal their personal information.

Here are the ways you can protect yourself:

- Think twice: check the activity on your bank account or phone us if you feel it could be a smishing attempt
- Do a quick web search. If it’s a scam, the chances are you are not the first person to receive that kind of message.
- If you’re still unsure about the legitimacy of the message, ask the opinion of a friend or family member, or speak with our support team in the app.
- If the message is a scam, block the number, delete the message from your phone and report the message to the support team at Pleo.