

Customer Security and Fraud Awareness Website Communication

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:

Logging into your account

We make use of Google Authenticator and Authy for 2FA (2 factor authentication), specifically TOTP (time-based one-time password). You are signing into your account with your self-created password and verified email address as username, ensuring a security system that requires two separate and distinct forms of identification to access your account. This also prevents anyone using your account from a previous session.

Verified details

Your account username, which is your email address, will be verified.

Limited User Data Collection

We prioritize transparency and minimalism when it comes to user data collection. We only gather essential information necessary for providing our services effectively. This includes basic user details such as name, email address and telephone number. Rest assured, we do not collect any additional unnecessary data.

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 [telephone number] [email address][in app notification].

Reporting Fraud: info@payselect.de

Lost or Stolen Cards: **069 348 73 76 0**

Suspicious Emails: info@payselect.de

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. A genuine company will never rush you to take action.

Always make sure your mobile telephone number and email address registered with us is up to date, 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 one-time passwords 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.
- When entering your PIN, check for people around you and hide your PIN number.
- Always check your statements.

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.