

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.

Memorable Questions – If you contact our customer services team, we may ask you to confirm who you are by asking you the memorable question responses you provided when creating your online e-money account.

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 by calling us or using the in-app chat.

Reporting Fraud: 03330 151 858

Lost or stolen cards: 03330 151 858 followed by option 3

Suspicious emails: hello@suitsmecard.com

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 card.

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

When accessing your Suits Me account:

- Use an antivirus software and firewall.
- Make sure you keep your device is up-to-date.
- Use secure networks.
- Use strong passwords.
- Don't share any passwords including pin or emoji login codes.

When using a mobile application:

- Only install apps from recognised app stores.
- Consider the app rating 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 websites 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, 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.