powered by tendris and sodexo

# 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.

**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 servicedesk, 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.

**One time passcode**

We send these unique one time use codes to your email address, provided by your company's administrator, for added security:

- periodically at login just to make sure it is you;
- when you request to make changes to your personal details.

**Providing information**

We will never ask you for your online password details or PIN number. We will always ask you to use our Milo app or selfservice website.

## 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 following contact details.

| | |
|---|---|
| Reporting Fraud: | servicedesk@xximo.de or 0180 6 – 555333* |
| Lost or Stolen Cards: | 0180 6 – 555333* |
| Suspicious Emails: | servicedesk@xximo.de or 0180 6 – 555333* |

* 35 cents/call from German fixed telephone network, max. 60 cents/call from mobile phones

## 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 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 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.