

# Your Security and Fraud Awareness

## Your security

Keeping your personal and financial information secure is our priority and when you access your Lix FX account, it's important that we know that it's you. Here are some of the measures we have in place:

- Providing Information – We'll never call or email you asking for your Lix FX account details, your one-time passcodes or passwords. If you do receive a call asking for this information, simply end the call and get in touch with us directly.
- Log in details – when you open a Lix FX account, you'll set up online login details unique to you. These will be your email address and password, to protect yourself we recommend you do not share them.
- Strong Customer Authentication (SCA) – The introduction of SCA legislation by the EU in 2019 require Lix FX to apply Strong Customer Authentication when you access your account. This means that you will have to enter your password (known only to you) and a code that we will send to either your registered mobile phone or your registered e-mail address.

## Keeping your money safe

- Lix FX is regulated by the FCA as an authorised payment institution (FRN: 526884)
- We hold your funds in specially designated bank accounts, which keep your money separate from our other assets. Where necessary, we safeguard any funds which will be used for a payment purpose. This means your monies are protected. However, these accounts do not fall under the Financial Services Compensation Scheme, for which only UK banks are eligible.

## Protecting yourself from fraud

Scammers and cybercriminals are more sophisticated than ever. Here's our top tips on keeping yourself safe from fraudsters.

When accessing your Lix FX account online:

- Use secure networks
- Use a strong password
- Never share or give out your personal details
- Use an antivirus software and firewall
- We'll never call or email asking for your account details, passcode or password
- Be aware of police advice on fraud threats - [here is an overview](#)

When online:

- Look out for bogus websites. You should always see this in the browser address window with a padlock icon being displayed. This confirms the page you are visiting is secure.
- When sending money to a new supplier for the first time, do some research to make sure that they are genuine
- Be aware of phishing emails and do not click on any suspicious links
- Protect your children online with parental controls and being vigilant
- Be vigilant on social media and oversharing personal information
- Be aware of authorised push payment fraud – these scams happen when a person or business is tricked into sending money to a fraudster posing as a genuine payee
- Use store apps when shopping on mobile devices

### **Reporting fraud**

If you notice something suspicious when using our platform and believe it could be fraudulent, we recommend getting in touch with us as soon as possible:

- **Telephone:** 0208 343 1188
- **Email:** [info@lixfx.com](mailto:info@lixfx.com)

Generally, if you think you've uncovered a scam, been targeted by a scam or fallen victim to fraudsters, contact Action Fraud on [0300 123 2040](tel:03001232040) or at [Action Fraud](#).