



Below we outline some important safety information in order to help TFI Pay Portal Users protect themselves from fraud.

TFI Markets Ltd will never ask you for any personal details through telephone calls, emails, pop up windows and banners. Never reveal through the telephone, internet, email or any other media your personal details such as the Online portal PIN, Token codes etc.

TFI Markets Ltd, when it needs to verify your identity for purposes relevant to access to the Online portal (such as if you request to reset your PIN or unlock your account), will only request for the following information:

- Phone PIN
- ID number
- Username

PIN security

Never share your Online Portal PIN and/or Phone PIN and never leave it in an area that is not locked or secured. It is essential that users keep their Online Portal PIN and/or Phone PIN private and immediately report to TFI Markets any suspected security violation or PIN being compromised.

General computer security

- Update your software (operating system and other installed software) frequently to ensure you have the latest security patches.
- Maintain an active and up-to-date antivirus protection provided by a Reputable vendor. In addition to real-time scanning, schedule regular scans of your computer.
- If you suspect your computer is infected with malware, discontinue using it for activities involving sensitive information until the issue is resolved.
- Use firewalls.
- Require a password to gain access. Log off or lock your computer when not in use.
- Always lock your computer when away.

General online security

- Never click on suspicious links in emails, posts, tweets or other online advertising.
- Only provide sensitive information to websites using encryption so your information is protected as it is transmitted across the Internet. Verify the web address begins with "https://" rather than "http://"
- Do not trust sites with certificate warnings or errors
- Avoid using public computers or public wireless access points for activities involving sensitive information
- Always "sign out" of password protected websites when finished
- Be cautious of unsolicited phone calls, emails or texts directing you to a website or requesting sensitive information.

Other important considerations for Companies

- Limit unnecessary web surfing and/or email activity by employees, including personal activity on computers used for online payments.
- Educate company personnel on good cyber security practices, clearing the internet browser's cache before and after visiting a financial institution's website.
- Consider assigning roles to separate duties in a company. For instance, one user can enter payment instructions on a transaction and another can approve it.