

Security Guidelines



TOTALITY

Totality is committed to safeguarding our clients by implementing risk mitigation measures to secure your account. To uphold our stringent security standards, as well as those mandated by regulatory bodies governing our industry, Totality prioritises the safeguarding of the trading platforms utilised by our clients. In addition to our efforts, it is essential for you to understand how you can contribute to maintaining and enhancing the security around your investment account.

2FA: Enhancing Your Trading Platform Security

Two-Factor Authentication (2FA) is a security measure that verifies a user's online identity using at least two different types of authentication factors from the following categories: "something you know," (e.g. password or pin) "something you have," (e.g. phone including WhatsApp, email or sms code or security token) or "something you are." (e.g. facial recognition or fingerprint).

2FA is designed and incorporated to protect your account and information from unauthorised access, while enhancing the overall security of online trading systems.

Totality requires all clients to use 2FA to ensure the security of their accounts. When accessing an online service provided by Totality, clients must enter their password and a One-Time Password (OTP), which may be delivered via WhatsApp, SMS, or email. This compulsory process provides an additional layer of security, safeguarding your trading activities.

Further Protection When Trading Online

To secure your password, personal details, and other confidential data, observe the following practices:

1. Credentials Management:

- Use passwords with at least 8 alphanumeric characters.
- Avoid guessable information like user ID or personal details.
- Keep passwords confidential and memorised, changing them regularly.
- Use different passwords for different sites.

2. Browser and Website Security:

- Avoid storing usernames and passwords in browsers.
- Verify website authenticity and look for 'https://' and security icons.

3. Account Monitoring:

- Regularly check account information and report discrepancies.

4. Software and Device Security:

- Install antivirus, anti-spyware, and firewall software.
- Keep software updated with security patches.
- Disable file and printer sharing when online.
- Regularly back up critical data.
- Use encryption for sensitive information.

Security Guidelines



5. Safe Online Practices:

- Log off after each session.
- Avoid installing unknown software.
- Delete junk emails and avoid opening attachments from strangers.
- Do not disclose personal or financial information.

Beware of Social Engineering Be cautious of unusual requests or offers, as social engineering can lead to divulging confidential information. Never share account details verbally or in writing, and be sceptical of calls from individuals posing as Totality staff.

Is Your Computer Vulnerable?

Ensure your software is up to date to prevent attacks. Use antivirus software and enable firewalls to protect against malware.

Preventing Unauthorised Trading

Avoid reusing passwords across different sites. Use password management tools and create complex passwords for secure accounts. Change passwords regularly, especially for banking sites.

For any irregularities, contact us immediately for assistance.