Anti-Fraud Awareness & Security — https://bluestone-gate.com/

1. Stay Secure in the Digital Realm
   At https://bluestone-gate.com/, protecting your personal information, funds, and trading account is a top priority. In today's digital financial environment, fraudsters and identity thieves use increasingly sophisticated tactics — including phishing, fake websites, and impersonation — to try to access your details.

This section explains how to recognise threats and minimise the risk of fraud.

2. Recognising Fraud & Phishing Attempts
   Fraudsters often pose as legitimate companies to trick clients into revealing account credentials, passwords, or financial information. Be alert to communications that:

• Urgently ask you to take action that seems unusual or out of the ordinary for your account.
• Request personal information beyond what https://bluestone-gate.com/ would normally require.
• Contain suspicious links, attachments, or unfamiliar web addresses.
• Come from email addresses or phone numbers that don't match our official channels.
• Contain spelling/grammar mistakes or unrealistic promises (e.g., guaranteed profits).
• Direct you to unofficial websites that are not part of https://bluestone-gate.com/.

3. Protecting Your Personal Information
   To safeguard your account and data:

• Verify All Communications
Always double-check any email or message claiming to be from https://bluestone-gate.com/. We will never ask for your password or secure credentials via email.

• Use Secure Networks
Avoid logging into your https://bluestone-gate.com/ account over public or unsecured Wi-Fi networks.

• Keep Passwords Confidential
Do not share passwords or 2FA (two-factor authentication) codes with anyone. Do not reuse passwords across platforms.

• Enable Two-Factor Authentication (2FA)
Activate 2FA on your account — this adds an extra layer of security to prevent unauthorised access.

• Keep Devices Updated
Ensure your devices, operating system, and antivirus/security software are up to date to protect against emerging threats.

• Official Channels Only
Always access your account through the official https://bluestone-gate.com/ website or authorised mobile app. Do not use links from unsolicited messages or unfamiliar social media channels.

4. What https://bluestone-gate.com/ Will Never Do
   https://bluestone-gate.com/ will:

• Never ask for your login password or 2FA codes via email or text.
• Never proactively call you without prior agreement to request sensitive information.
• Never send offers that guarantee trading profits or returns.
• Never send you to unofficial duplicate websites to “claim rewards” or “verify your account.”

If you receive a suspicious message claiming to be from us, do not click any links or enter personal details. Contact https://bluestone-gate.com/ support immediately through official channels.

5. If You Suspect a Scam
   If you believe you have received a fraudulent communication or encountered a fake website:

Do not provide any personal or login information.
Do not click on any suspicious links.
Take a screenshot of the message and sender details.
Contact https://bluestone-gate.com/ support immediately for verification and assistance.

6. Your Responsibility
   You play an important role in protecting your account. Regularly review your security settings, update passwords periodically, and stay informed about common online threats. https://bluestone-gate.com/ provides tools and guidance, but you are ultimately responsible for maintaining the security of your login details.