
FRAUD RISK WARNING

At Columis, your safety and trust are our top priorities. Please take a moment to review the following guidelines to protect yourself and your assets.

1. Stay Cautious of Unsolicited Offers

Be wary of unsolicited contacts offering investment opportunities, trading services, or guaranteed returns claiming to represent Columis. Fraudsters may impersonate our brand or employees. Always verify the legitimacy of any communication through our official channels listed on our website.

2. No Guaranteed Returns

Crypto assets investments carry significant risks, and Columis does not guarantee profits or returns. Promises of high or fixed returns with minimal risk are likely scams. Always approach investments with caution and conduct thorough research.

3. Protect Your Data

Columis will never request your private keys, passwords, or full seed phrases. Never share sensitive login or wallet details with anyone, even if they claim to be from our support team.

4. Verify Official Communications

Ensure all communications come from Columis' verified channels. Check website URLs (e.g., <https://www.columis.com>), email addresses (ending in [@columis.com](mailto:info@columis.com)), and contact details. If you receive an email with links requesting login credentials, do not click them. Instead, visit our website directly or contact us via our official support page: Contact Support.

5. Self-Custody Wallets

If you're using a self-hosted wallet, make sure you are the sole controller and have applied strong authentication measures (e.g., passwords, biometric verification). We are not responsible for losses caused by compromised third-party wallets.

6. Understand Your Obligations and Transaction Authorisations

By using our services, you agree to the terms outlined in our framework agreement, available at Terms and Conditions. This includes understanding how your consent is given for transactions, such as transfers to/from digital wallets, which require specific authorisation methods. Please keep in mind that crypto-asset transactions are generally irreversible.

7. Be Aware of Legitimate Requests for Information

In certain cases, such as requests to increase transaction limits, Columis may contact you to verify your identity using confidential personal information (e.g., ID number). However, we will never ask for personalised security data like passwords or private keys. If unsure, contact us directly to confirm the request via info@columis.com.

8. Report Suspicious Activity

If you encounter fraud, phishing attempts, or unauthorised use of our brand, report it immediately to our team at info@columis.com. If you've been a victim of fraud, contact us promptly, and we'll provide guidance on next steps based on the latest security threats and vulnerabilities.

9. Our Commitment to Your Security

Columis regularly tests and assesses our authentication tools and services to mitigate fraud risks. We provide ongoing support to address your questions and concerns about payment service security.

10. Stay Informed About Service Updates

We may update our systems or terms of service to enhance security and functionality. Notifications about such changes will only include links to publicly available information (e.g., "read more" links to our website). We will never ask you to log in via links in emails or other electronic communications.