

Phishing Awareness Quick Reference

Disclaimer These materials are internal BTC guidelines for awareness and consistency. They are not a contract, promise, or guarantee of specific outcomes. BTC may interpret, modify, or suspend this guidance at any time. Where law, partner requirements, or a signed agreement require different handling, that requirement controls. Questions or exception requests: support@bigthinkcapital.com.

Quick Red Flags - Unfamiliar sender or domain that looks close to a real one. - Urgent tone or threats if you do not act immediately. - Links that look unusual. Hover to preview the real destination. - Requests for credentials, wire transfers, gift cards, or confidential info. - Unexpected attachments or voicemail links.

What To Do - Do not click. Take a breath and look carefully. - Report the message using any available Report Phish option or forward to support@bigthinkcapital.com. - If you clicked, change your password and email support@bigthinkcapital.com so the team can help.

Everyday Habits - Keep devices updated and use MFA. - Use managed storage and links for sharing files. - Ask for a second opinion whenever something feels off.

Exceptions If a team needs to deviate from this guidance, email support@bigthinkcapital.com with the context, risk, and temporary controls. Keep exception decisions in writing.