SOP E — ‘Is This Phishing?’ Quick Triage

ToroTek LLC — Standard Operating Procedure

A 2-minute check to avoid bad clicks. When in doubt, verify using your normal login route—never the link in the message.

Before You Start

- Create a reporting email/Slack channel for suspicious messages.
- Have staff bookmarks for real sites (bank, email, e-signature).

Step-by-Step

1. **Step 1.** Pause: do not click links or open attachments.
2. **Step 2.** Check the sender’s address carefully; hover links to preview the destination URL.
3. **Step 3.** Look for urgency tricks (‘account locked’, ‘payment due’, gift cards).
4. **Step 4.** Verify by opening the real site from your bookmark and signing in there—ignore the message link.
5. **Step 5.** Report the message to the firm lead or IT; then delete it.

Done-Right Checklist

- No one clicked or entered credentials.
- Suspicious message forwarded to IT/security for review.
- Sender or domain blocked if confirmed phishing.

When to Call ToroTek

- Someone clicked the link, opened an attachment, or entered credentials.
- Unexpected MFA prompts or password reset emails appear.
- Antivirus/EDR flags new activity on the device.

If Someone Clicked

- Immediately change the account password and enable/confirm MFA.
- Scan the device with EDR/antivirus; review mailbox rules for rogue forwards.
- Notify IT/management; document the event in the incident log.

Need help? ToroTek is here.
Call/Text: 619-376-6995
Support: help@toro-tek.com
Web: torotekllc.com

Updated: 2025-08-13