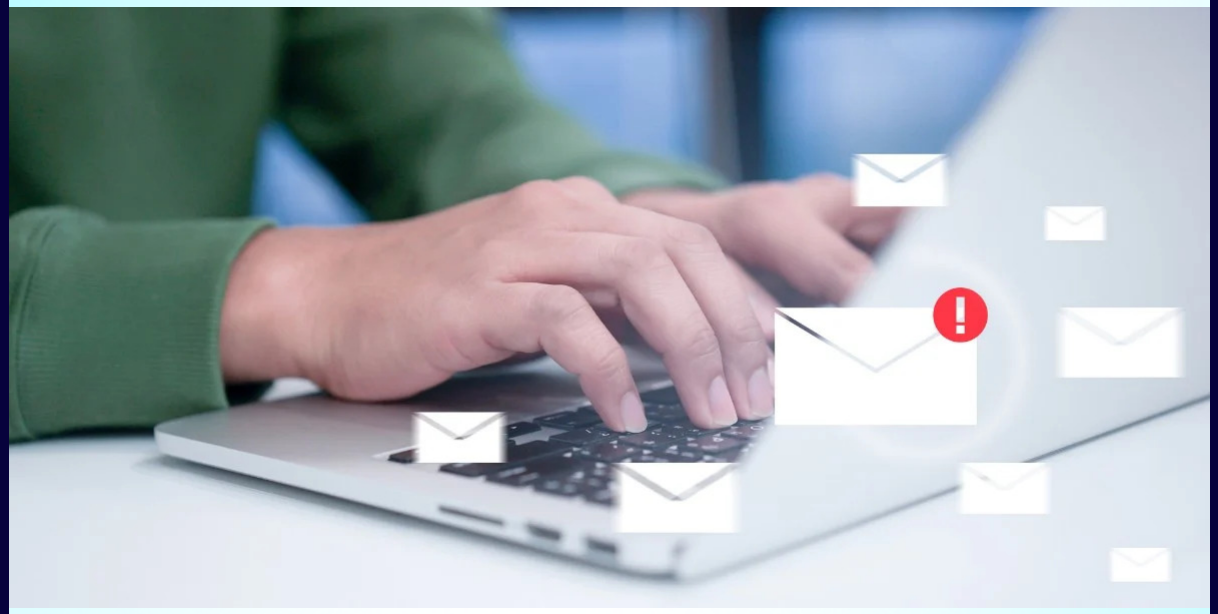
How to spot AI phishing attempts and other security threats

Your Quick Guide to Cybersecurity Awareness

In the fast-evolving digital landscape, AI-enhanced phishing and cyber threats are becoming more sophisticated. As your trusted IT partner, we're committed to keeping you informed and prepared.



Here's what you need to watch for:

- **Unusual Email Patterns:** AI phishing often involves emails that are too perfect — impeccable grammar, precise vocabulary, and tailored content. Be wary of messages that seem unusually well-crafted or overly personalized, especially if unexpected.
- **Sender Verification:** Always double-check email addresses and domains. Look for subtle misspellings or odd character replacements. Cyber criminals often mimic legitimate contacts with only minor alterations.
- **Context and Urgency:** AI attackers exploit urgency and context. If an email pushes for immediate action or leverages recent events to seem credible, take a moment to verify its authenticity.
- **Analytical Vigilance:** Employ tools and techniques to scrutinize email origins and contents. Be skeptical of any links or attachments and hover over links to preview URLs.

Need Help?

Contact Us Now

Your proactive stance is crucial. By staying alert to these signs and adopting robust security measures, you can significantly mitigate the risk of falling victim to these advanced threats. Stay safe, stay informed, and together, we'll continue to safeguard your digital landscape.

Stay Secure,
The Click IT Team

For Customer Care Support
Call (440) 247-4998

Or email support@clickitco.com