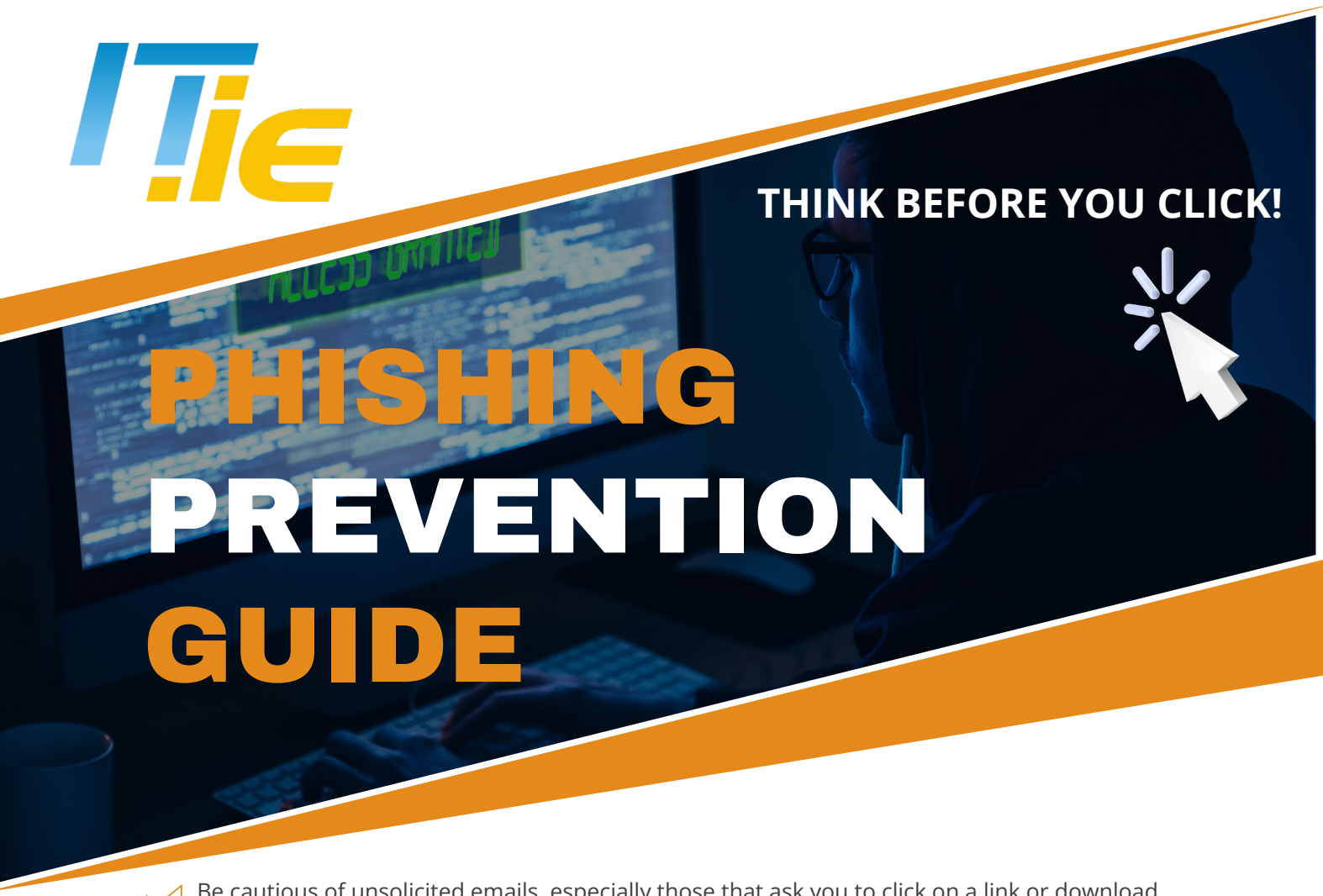

THINK BEFORE YOU CLICK!

PHISHING PREVENTION GUIDE

- Be cautious of unsolicited emails, especially those that ask you to click on a link or download an attachment.
- Look for suspicious email addresses, such as ones that use your company's name in an unfamiliar way or ones that are from a free email service.
- Pay attention to the email's subject line and tone. Phishing emails often have urgent subject lines and a sense of immediacy to try to get you to act quickly.
- Check the sender's email address carefully. Sometimes, phishers will use an email address that is similar to a legitimate one, but not exactly the same.
- Be wary of links in emails. If you hover your cursor over a link, your email client should show you the true destination of the link. If it looks suspicious, don't click on it.
- Use antivirus software and a firewall to protect your IT systems.
- Keep your software up-to-date. Many software updates include patches for security vulnerabilities, so it's important to stay current.
- Use Multi-factor authentication when it is available. This adds an extra layer of security by requiring you to enter a code that is sent to your phone or generated by a security app in addition to your password.
- Employ a Cyber Awareness Training service to educate your team about phishing attacks and how to recognise them. This can help prevent someone in your organisation from falling victim to a phishing attack.
- If you receive an email that you think might be a phishing attempt, don't respond to it and don't click on any links or download any attachments. Instead, report the email to your IT department or your IT Support provider.

+353 18424114 hello@it.ie www.it.ie