Quick Response Guide for Phishing Email

Spot the Phish ("Is this real?")

- Unknown sender – address doesn't ring a bell.
- Urgent tone – "Act now," "Verify immediately," prizes or penalties.
- Sloppy language – misspelled words, odd grammar, off-brand logos.

If two or more of these flags appear, treat the message as a phishing attempt.

Pause - Do NOT Interact

- Don't click links or attachments.
- Don't follow phone numbers or instructions in the email.
- Don't reply - replying confirms your address is active.

Report

- Work account: forward to your IT/Security team per policy.
- Personal account: use the mail-client "Report phishing" option.
- National authority (e.g., IC3 in the U.S.), if available.

Delete Safely

- Remove from Inbox and Trash/Deleted Items.
- Never forward the message to colleagues.

Prevent Future Hits

- Keep anti-malware and email filters updated.
- Enable MFA wherever possible.
- Regular security awareness training for all staff.
- Businesses: review your email-security stack and incident-response playbooks.

Visit www.ampcuscyber.com or reach out to us at letsconnect@ampcuscyber.com