Protect Yourself from Phishing Scams

Don't be the next victim—Learn how to stay safe now!

Common Signs of Phishing

Urgent or Threatening Messages: Messages urging immediate action.

Unknown or Suspicious Senders: Emails from unknown or suspicious sources.

Poor Grammar or Generic Greetings: Impersonal messages with poor grammar.

Mismatched Email Domains: Emails from odd domains or slight misspellings.

Suspicious Links or Attachments: Hover over links to verify before clicking.

Fake Order Scams: pretend to be order confirmations or invoices.

Actions to Take

Don't Click Any Links or Open Attachments: Verify first.

Verify the Sender: Use official channels to confirm legitimacy.

Report the Message: Use "Report Message" in Outlook or Teams or contact your local IT administrator.

Delete the Suspicious Message: After reporting, remove it from your inbox.

If You Think You've Been Phished:

Change All Affected Passwords immediately

Enable Multi-Factor Authentication (MFA)

Contact Your Bank or Credit Card Company

Report to Local Authorities

www.ProServeIT.com | cloud@ProServeIT.com | @ProServeIT

PROSERVEIT