



STOP! THINK BEFORE YOU ACT.

Phishing could be considered the biggest threat to business security worldwide. But it can be thwarted with your awareness. Think before you act.

Phishing uses a specific company or individual's likeness to trick employees into revealing confidential information, and it comes in various forms – via email, telephone, and social media.

✓ DO

Do use filters

Use spam filters and updated protections.

Do be cautious

Be cautious with all email attachments no matter who they are from.

Do verify links

Mouse over links to verify they lead to the correct website urls.

Do verify contacts

Verify the identity of contacts by checking email addresses and telephone numbers.

Do be mindful

Be mindful of social media responses to your inquiries; they may come from fraudulent accounts.

⊘ DON'T

Don't click links

Don't click links or attachments if you don't recognize the sender.

Don't respond

Don't respond to suspicious, out-of-character messages.

Don't give access

Never respond to requests for personal identification or access information.

Don't reveal

Never reveal your personal banking details; keep your PIN and CVV numbers private.

Don't click on popups

Don't click on popup windows because they may redirect you to a fraudulent site or download malware.