

# Phishing Checklist

## CHECKLIST INSTRUCTIONS

Fold or cut the quick checklist on the right. Place it somewhere you can see when reading your emails. Read the rest of this document to better understand each checklist item.

## RESPONSES

### Not sure if it is phishing?

Navigate to the information on your own. Any legitimate company will have a way outside of clicking an email link. -OR- Search online for more information to support your choice to click or ignore. -OR- Contact the sender (if trusted) through another method (e.g., phone call, text message, etc.) to verify before clicking.

### Are you sure it's phishing?

Mark the message as junk, block the sender email address, and permanently delete the message.

### Did you click a phishing link?

Report it to ISO/IT immediately. Clicking was a mistake, hiding it is willful harm to the company.

## CLUES

Clues are things which are clearly wrong with the email.

### Links and Attachments

Are you being asked to click a link or open an attachment? Does hovering over the links show the expected destination URL?

### Errors

Is the message unprofessional or covered with typos and grammatical errors?

### Unfamiliar Sender

Do you recognize the name and email address of the sender? Is the domain similar, but not quite right?

### Familiar, yet Unusual

Is your contact using an unusual salutation, tone, signature, or sending at a strange time of day?

### Unexpected Email

Is this email "out of the blue," or is it a "follow up" on a request you did not make?

### Personal Topics

Is the message of a personal nature (e.g., taxes, shipping, appointments, etc.)? Do you use your work email for personal communications?

## MY PHISHING SECURITY AWARENESS CHECKLIST

### Check for clues.

- Links / Attachments
- Unfamiliar Sender
- Unexpected Email
- Errors
- Familiar, yet Unusual
- Personal Topics

### Beware of tactics.

- Urgency
- Loss
- Authority
- Familiarity
- Reciprocation
- Popularity

### Respond appropriately.

- Not sure?** Navigate on your own, do some research, or ask the contact through another method.
- Sure?** Mark as junk, block, and delete.
- Clicked?** Report it immediately. Clicking was a mistake, but hiding it is willful harm to the company.

### Thank you!

Falling for a phishing attack can harm the company's reputation, financials, systems, and hinder our ability to serve our clients. We appreciate your help and dedication!

## TACTICS

Tactics are distractions to make you act without thinking.

### Urgency

Phrases like "required" and "today" are designed to make you rush.

### Loss

Language about losing access to something is designed to make you worry.

### Authority

Posing as your boss, HR, or other authoritative group is designed to make you blindly obey.

### Familiarity

Using publicly available information about you is designed to make you assume familiarity.

### Reciprocation

Offering you something is designed to make you feel obligated to give something in return.

### Popularity

Language about other people doing something you're not is designed to make you feel wrong.