

# Information Security Training

Internal use

# PHISHING

## What is Phishing?

- Phishing is a type of Social Engineering attack
- Unlike other security attacks, it leverages you by sending you a fake email that tricking you click on a link or open some attachment
- Clicking on a link may take you to some bogus site where you maybe asked to enter sensitive information such as a user name and password
- Opening an attachment may be malware in disguise waiting to be installed

# Social Engineering Red Flags

## HOW TO IDENTIFY A PHISH?

- Usually an unexpected communication
- Comes from some person or company you are familiar with
- Subject is usually related to money or some account
- Misspellings in the address, content, greeting
- Mismatch of the sender name and email address
- Missing logos, contact info

## SOMETHINGS TO QUESTION

- Is there a sense of urgency?
- Is it asking you to click on a link or open an attachment?
- Is it asking you to input any sensitive information, account names, user IDs, passwords, etc.?

## FROM

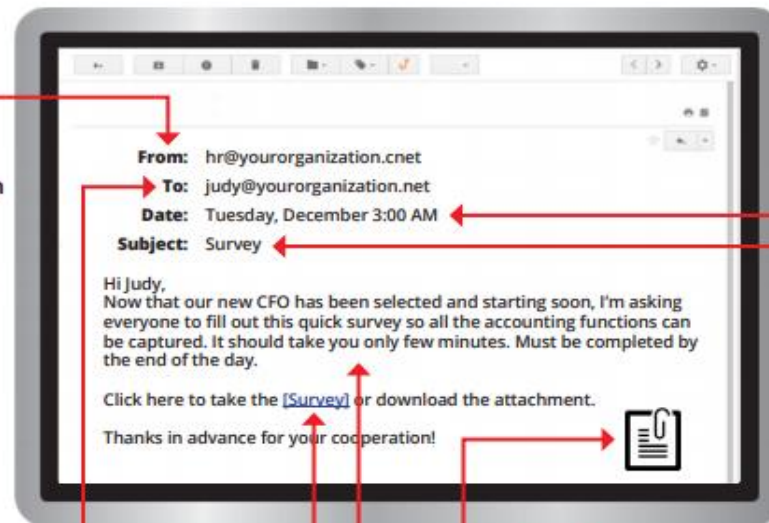
- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

## TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

## HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known website. For instance, [www.bankofamerica.com](http://www.bankofamerica.com) — the "m" is really two characters — "r" and "n."



## DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

## SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

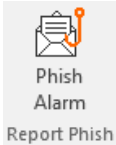
## ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**.

## CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

# WHAT TO DO IF YOU'VE BEEN PHISHED

- Don't click on any links or open any attachments
- Don't reply to the email
- Delete it
- Inform the Information Security Office by using the Phish Alarm button on the Outlook tool bar  or emailing [\\_ITSecurity@tmmc.com](mailto:_ITSecurity@tmmc.com)