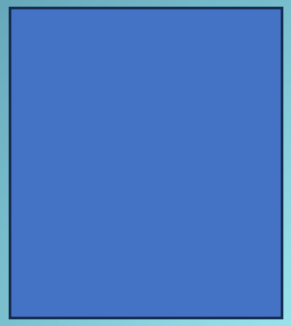
CenterPoint Energy

Cybersecurity Awareness –Safety Phishing Refresher

2023

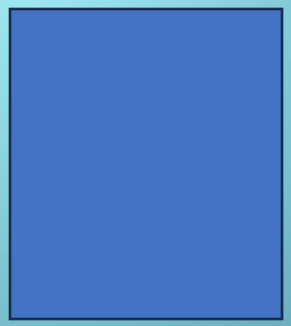
Introductions

Cybersecurity Awareness Team



Name
Title
Cybersecurity Awareness

Name
Title
Cybersecurity Awareness



Name
Title
Cybersecurity Awareness

Why do we phish?

We conduct campaigns to teach CNP employees to recognize red flags in malicious emails to prepare them for real malicious attempts

Campaigns also provide an opportunity to develop and practice their skills in order to recognize malicious emails and report them to the CSOC

Ultimately campaigns reduces the risk of employees falling victim to a social engineering attempts and **protects CNP!**

How to prevent fails

Phishing Indicators

Who is the email from?

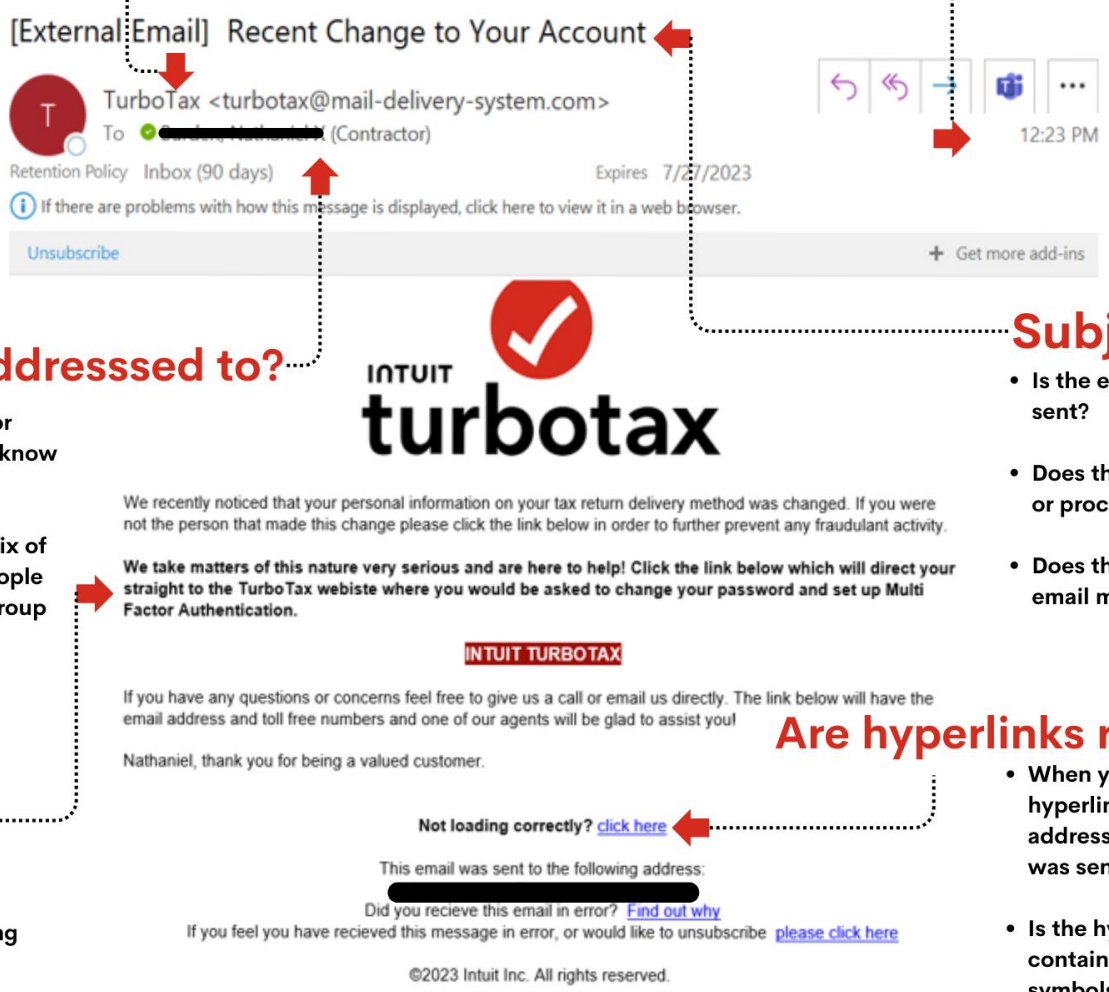
- I don't recognize the senders email as someone I ordinarily communicate with
- The email is from someone outside my organization and not related to my job responsibilities
- I don't have a business relationship with sender

Who is the email addresssed to?

- I was cc'd on an email sent to one or more people but I don't personally know the sender or other recipients
- The email was sent to an unusual mix of people. For example, a group of people with the same name or initial or a group of unrelated email addresses

Content

- Request for sensitive information
- Poor formatting, grammar or spelling mistakes
- Is the sender asking you to click on a link or attachment to avoid a negative consequence or gain something of value?



Verify Time and Date

- Was this email sent during regular business hours?
- Was the email sent at an unusual time?

Subject

- Is the email in reply to a message you never sent?
- Does the subject refer to an unknown topic or process?
- Does the subject match the content of the email message?

Are hyperlinks real and accurate?

- When you hover your mouse over the hyperlink that's displayed, is the link-to address different than the domain the email was sent from?
- Is the hyperlink misspelled or does it contain letters that are created with other symbols?

CYBERSECURITY AWARENESS

Scenario 1

Cyber Becky's Surprise Invoice

Cyber Becky opens her inbox to find an email titled "Urgent Invoice Due!" from "accounting@payfastt.biz". The email address doesn't match her company's regular billing department. The content of the email reads:

"Dear Valued Customer,

Please make an immediate payment of $1,500 for the services rendered last month. Click here to view the invoice and make a payment."

Would you advise Cyber Becky to consider this email as normal or malicious?

Scenario 2

Cyber Bob's IT Update

Cyber Bob receives an email from "support@hiscompany.com" with a subject line, "Important System Update." The content of the email says:

"Hi Bob,

We will be undergoing a system update this weekend. Please ensure you save all your work before leaving on Friday. If you face any issues, reach out to us.

Best,

IT Team"

Would you advise Cyber Bob to consider this email as normal or malicious?

CenterPoint Energy

Q&A

Thank you!!!