



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!**



\$4.35M

In 2022, the average cost of a data breach has reached a record high of US \$4.35 million

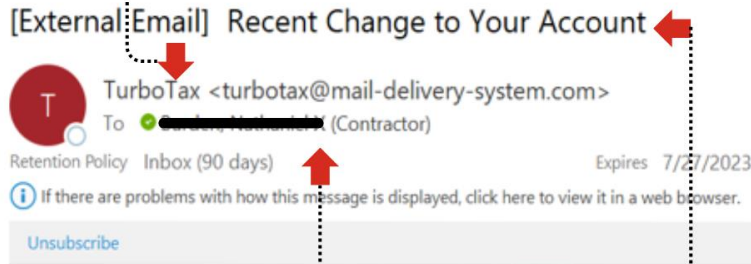
How to prevent fails



Phishing Indicators

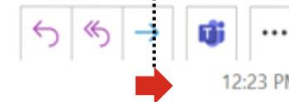
Who is the email from?

- 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



Verify Time and Date

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



Who is the email addressed 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



We recently noticed that your personal information on your tax return delivery method was changed. If you were not the person that made this change please click the link below in order to further prevent any fraudulent activity.

We take matters of this nature very serious and are here to help! Click the link below which will direct your straight to the TurboTax website where you would be asked to change your password and set up Multi Factor Authentication.

INTUIT TURBOTAX

If you have any questions or concerns feel free to give us a call or email us directly. The link below will have the email address and toll free numbers and one of our agents will be glad to assist you!

Nathaniel, thank you for being a valued customer.

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?

Not loading correctly? [click here](#)

This email was sent to the following address:

Did you receive this email in error? [Find out why](#)

If you feel you have received this message in error, or would like to unsubscribe [please click here](#)

©2023 Intuit Inc. All rights reserved.

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?



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?



Q&A
Thank you!!!