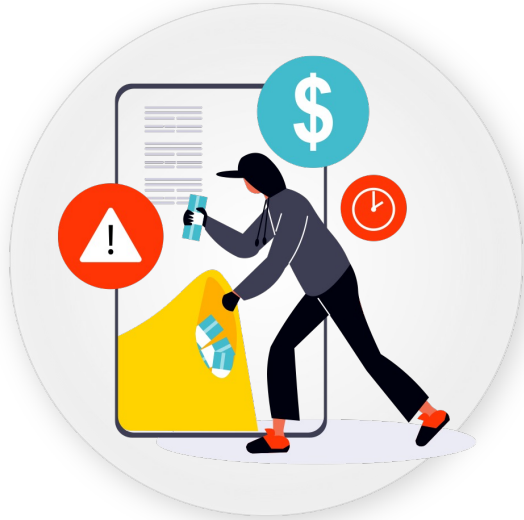


RECOGNIZE & REPORT PHISHING

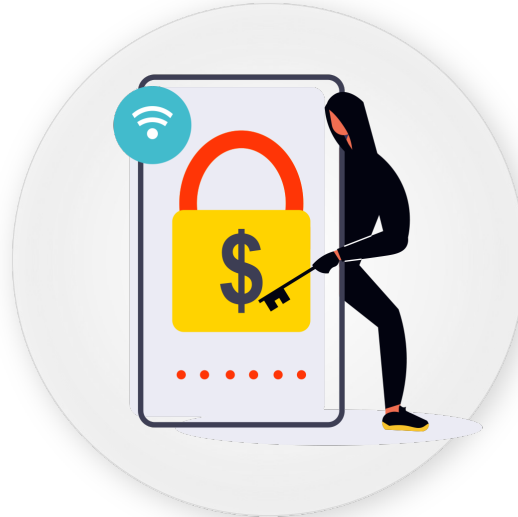
Do Your Part. [#BeCyberSmart](#)



RECOGNIZE: What is Phishing?



URL LINK



CREDENTIAL

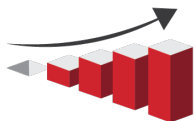


ATTACHMENT

RECOGNIZE: Business Email Compromise [BEC]



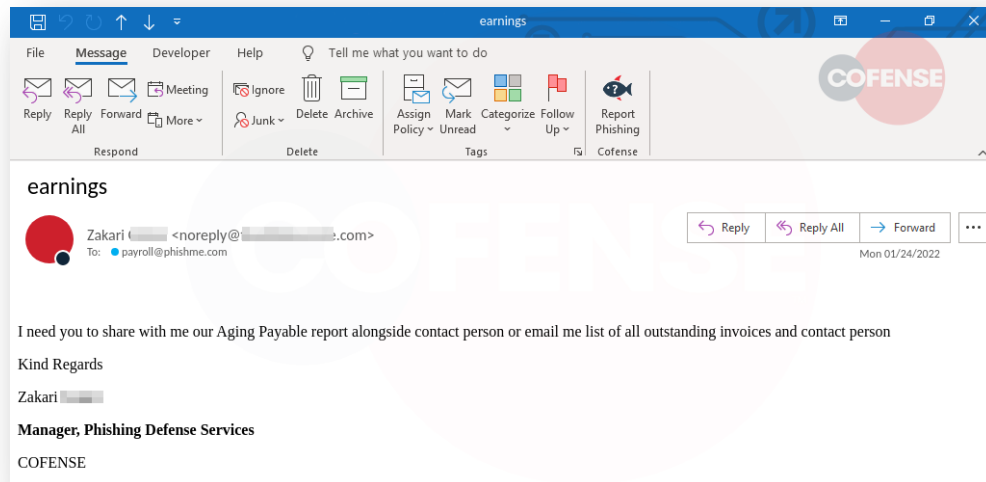
No URL to click or Attachment to open



\$43+ B 2021 (IC3.gov)



- Impersonate legitimate person of authority within the organization
- Request Gift Cards
- Direct Deposit Changes



RECOGNIZE: Business Email Compromise [BEC]



Always Observe Policy



**Always check the sender
and verify its legitimacy**



**Always Check Reply-to
Addresses**





RECOGNIZE: Indicators of a Phish

1. **Unknown Sender**
2. **Emotional Appeal**
3. **Spelling/Grammatical Errors**
4. **URL Link**
5. **Solicits Sensitive Information**

The mockup shows an email header with a trash icon, two 'reply' icons (one purple, one blue), and a 'reply all' icon (blue). A fish icon with a question mark is in the top right. The email body contains the following text:

From: christopher.mccoy@intlpackagedelivery.com (1)

Subject: ATTENTION REQUIRED: TROUBLE WITH YOUR ORDER (2)

This is an automatic notification: you must go through this letter to claim the item. (3)

Follow the URL seen down below to use our recently implemented tracking system.

[Order 3251351](#) (4)

Enter your username password tracking number to verify the account. (5)

All the best,
Christopher McCoy - Chief Support Manager.

RECOGNIZE: Credential Phish

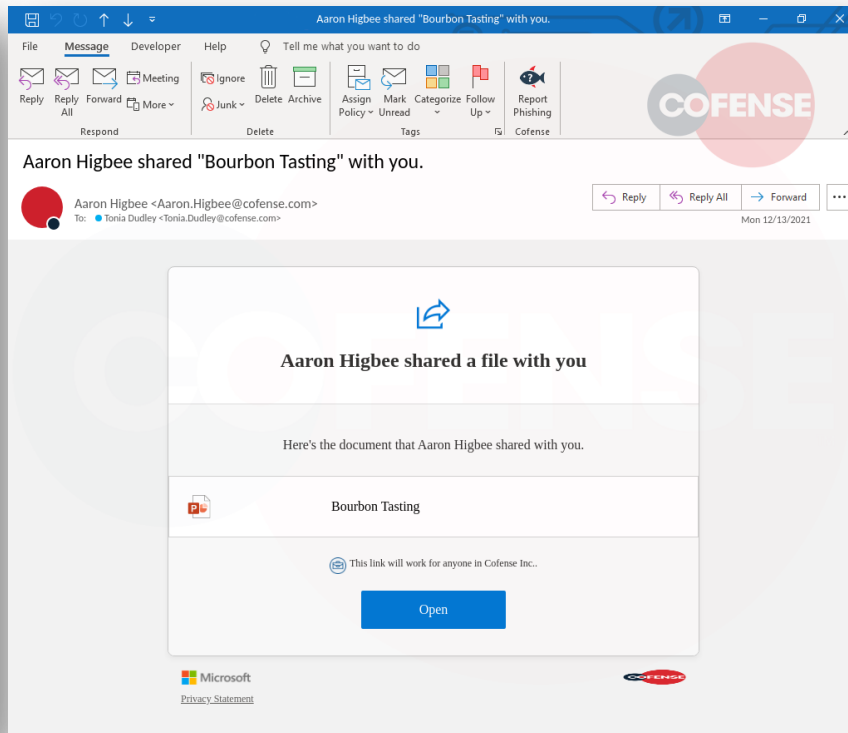
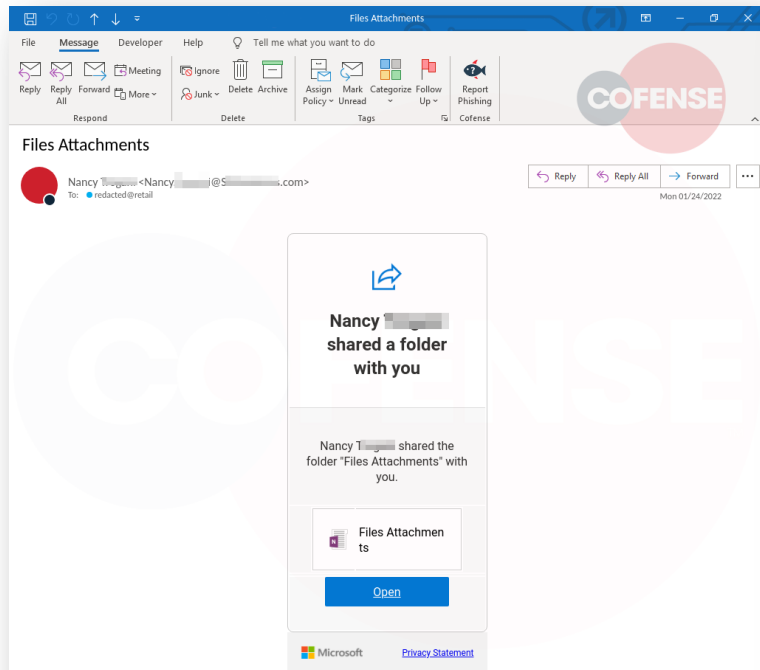


O365 Users - Threat actors often use compromised O365 accounts. Carefully review the email to determine if something doesn't feel right.



Personal Email – Threat actors often spoof banking websites and shopping sites. Be careful when accessing a portal via an email link.

RECOGNIZE: Credential via Link



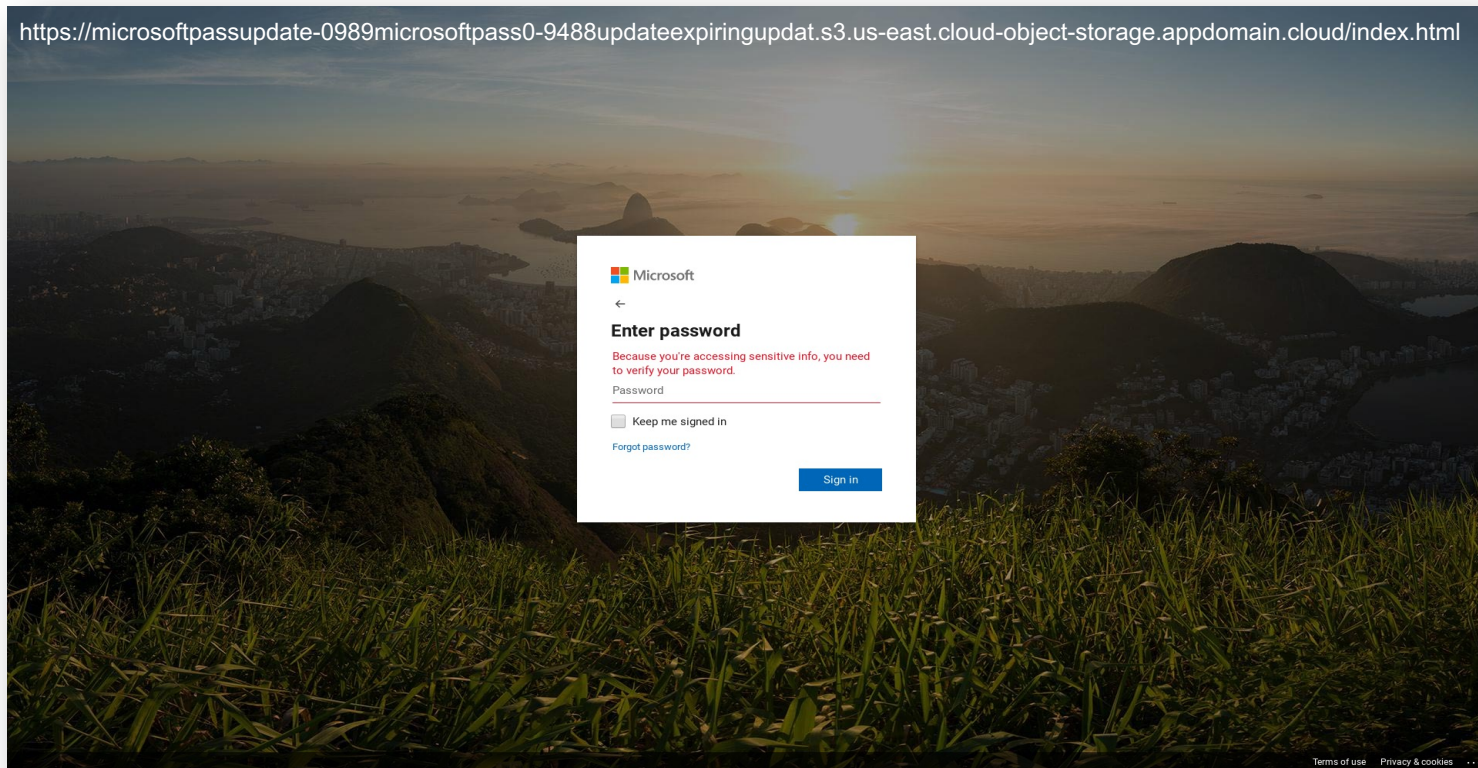
Tactic: Link | Threat: Credential Phishing | SEG: Proofpoint



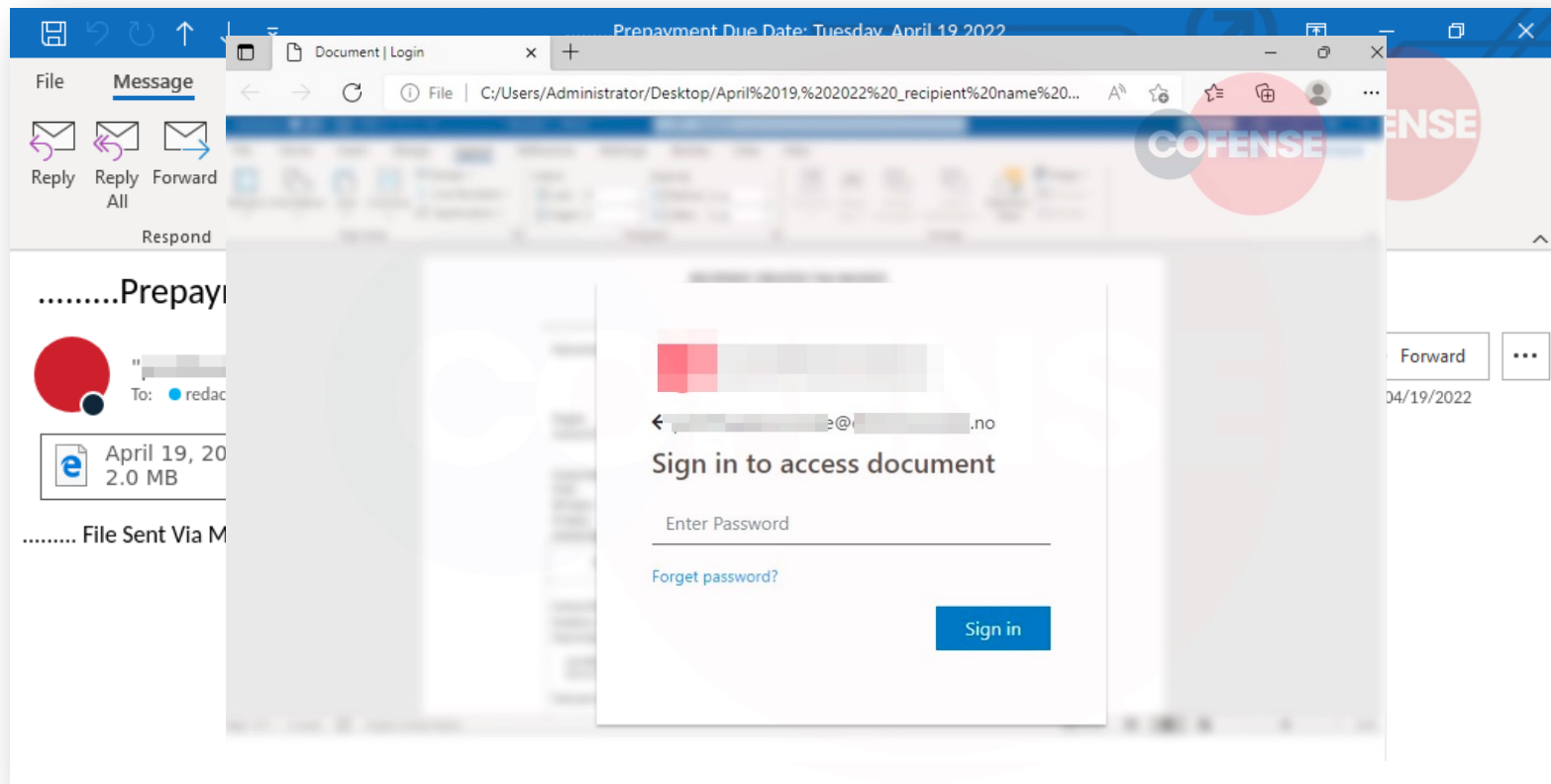
RECOGNIZE: Credential



<https://microsoftpassupdate-0989microsoftpass0-9488updateexpiringupdat.s3.us-east.cloud-object-storage.appdomain.cloud/index.html>



RECOGNIZE: Credential Phish via HTM File



RECOGNIZE: Credential Phish via Link



RE: [REDACTED] LTD 2022 PROJECT MEMO

File Message Developer Help Tell me what you want to do

Reply Reply All Forward Meeting Ignore Delete Archive Assign Mark Categorize Follow Up Report Phishing

Respond Delete Tags Cofense

RE: [REDACTED] LTD 2022 PROJECT MEMO

Joe [REDACTED]
To: Joe [REDACTED]

<https://microsoftloginoffice.myportfolio.com/>
Click or tap to follow link.

Reply Reply All Forward ...

Wed 04/13/2022

Good morning. I hope you are doing well and in good spirits!

Kindly review the planned 2022 RFP document shared with you and let me know if you would be willing to work with us on this project [MEMO2022-Document/0352366](#)

Due to the size of some of the electronic RFP documents, Our IT Dept has uploaded them to the "Adobe sharepoint" website.

If you or your team require any additional information, please feel free to contact me directly.
Thank you,

Joe [REDACTED]





RECOGNIZE: BEC – Direct Deposit

FileMessageDeveloperHelpTell me what you want to do

ReplyReply AllForwardMore

IgnoreDeleteArchive

AssignPolicyMark UnreadCategorizeFollow Up

Report PhishingCofense

RespondDeleteTagsCofense

Assist

Wendy <roberto. >@atching.com>
To: hr@phishme.com

ReplyReply AllForward...

Mon 05/16/2022

I can access the employee portal but I keep getting an error message every time I try to modify my direct deposit information. Can I just forward you a voided check or my new account details for you to update before the next pay circle.

Wendy

COFENSE

RECOGNIZE: BEC – Free?



REQUEST


File Message Developer Help Tell me what you want to do

Reply Reply All Forward Meeting More ▾

Ignore Delete Archive Assign Policy ▾ Mark Unread Categorize Follow Up ▾ Report Phishing

Respond Delete Tags Cofense

REQUEST

 "Elise [REDACTED]" <president1097@gmail.com>
To: Stephanie, [REDACTED]@e.com

Reply Reply All Forward ...

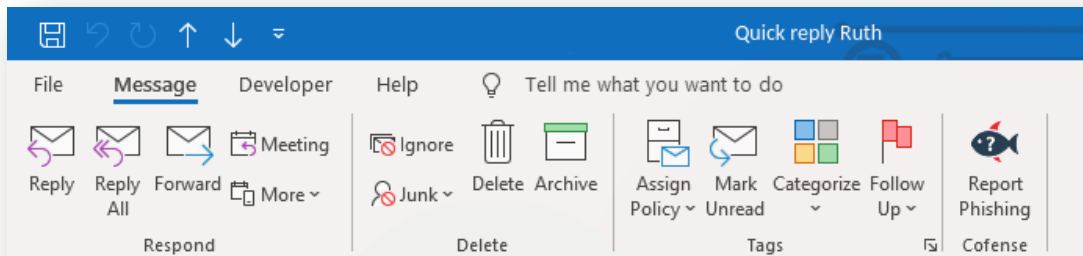
Sat 04/30/2022

Hi Stephanie,
Are you free at the moment in helping me out?

Best Regards
Elise [REDACTED]



RECOGNIZE: BEC – Gift Card



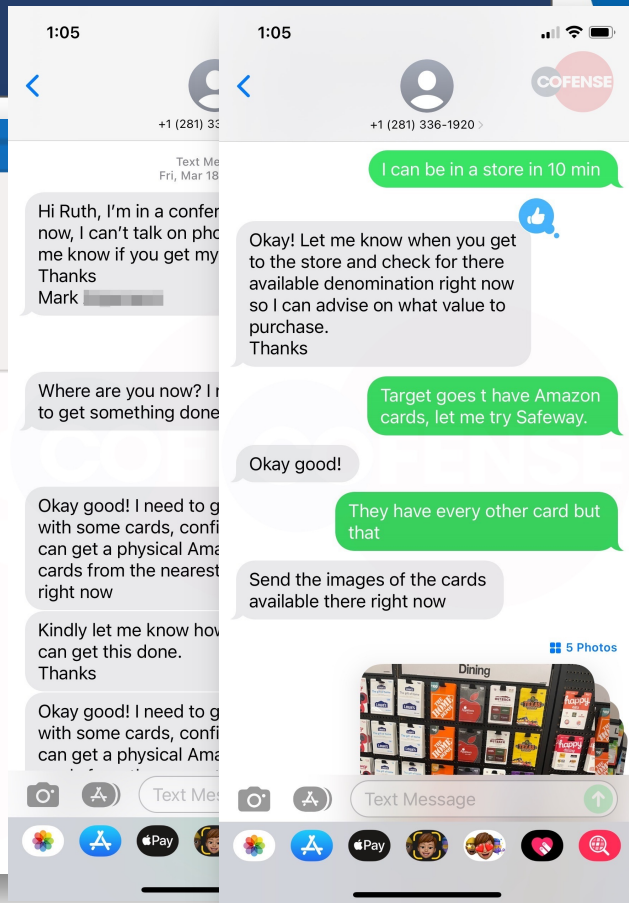
Quick reply Ruth



Mark [redacted] <[redacted]@paint@gmail.com>
To: Ruth [redacted] <[redacted]@[redacted].com>

Send me your personal mobile number, i need you to get something done.

Mark [redacted].
Best Regards,



COFENSE

RECOGNIZE: Malware via Link



Re: Not read: READINESS Document and Procedure: [REDACTED]

File Message Developer Help Tell me what you want to do

Reply Reply Forward Meeting Ignore Delete Archive Assign Mark Categorize Follow Up Report Phishing

Respond Delete Tags Cofense

Re: Not read: READINESS Document and Procedure: [REDACTED]

[Redacted Profile Picture] To: [Redacted]@[Redacted].com>

949.0 KB [Redacted]_071548.html

Good morning,

Below, I've provided the doc for your reference. Please remember to open the doc and give me some **feed-back**.

Please read this ASAP.

Thank you,

Your message

To: [Redacted] Mark [Redacted]
Subject: READINESS Document and Procedure: [REDACTED]
Sent: Friday, November 20, 2020 [REDACTED]

was deleted without being read on Monday, November 23, 2020 [REDACTED]



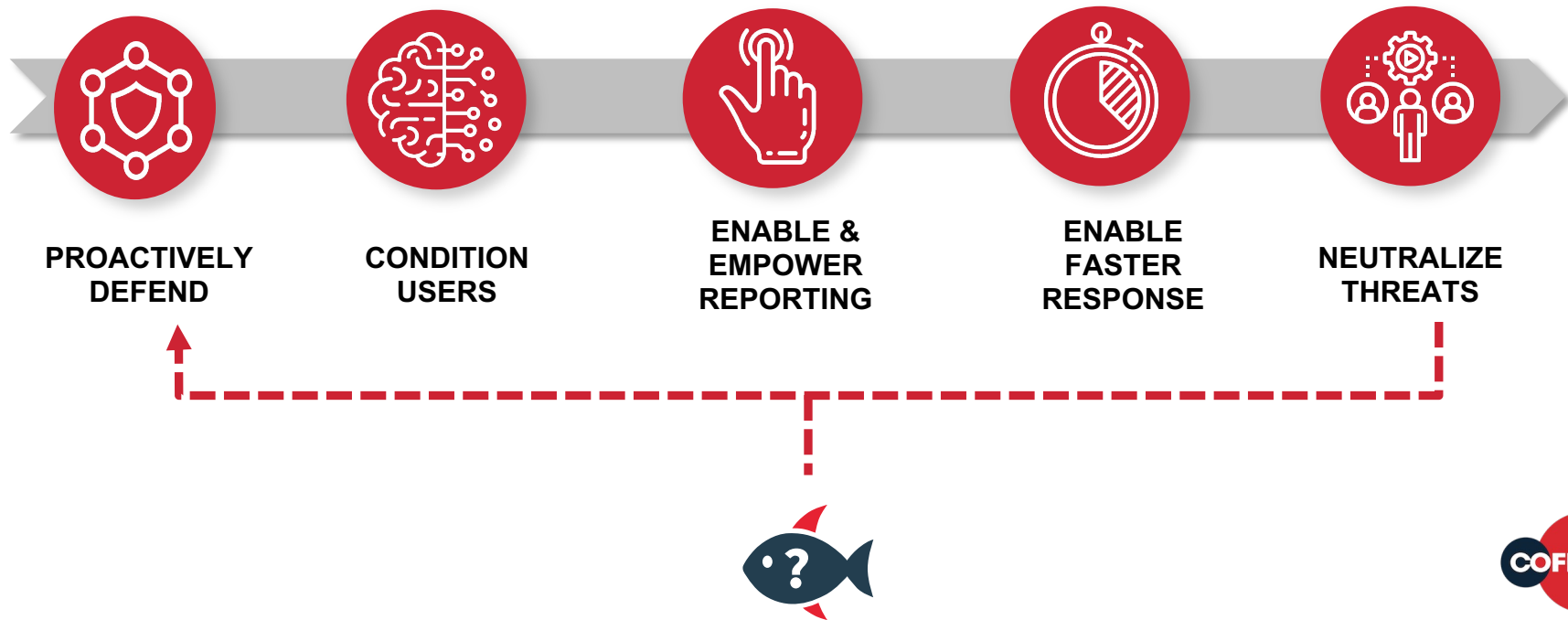
REPORT: What can we do?



Report the email



REPORT: Response Timeline



BE CYBER SMATER: @HOME



Create Unique Accounts



Password Vault

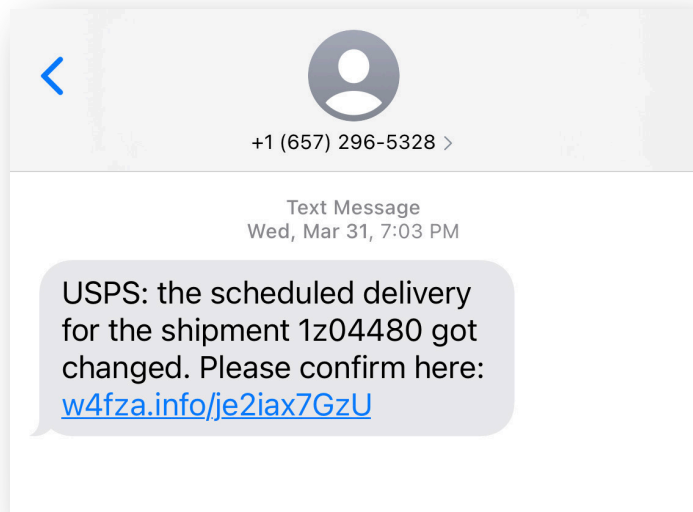


Enable 2FA

<https://2fa.directory>



BE CYBER SMATER: @HOME



REPORT: forward to **7726** (SPAM)

<https://staysafeonline.org/theft-fraud-cybercrime/reporting-matters-even-for-a-smishing-message/>



CYBERSECURITY IS EVERYONE'S JOB. INCLUDING YOURS.

LEARN HOW EASY IT IS TO STAY SAFE ONLINE.

#BeCyberSmart

ADDITIONAL RESOURCES



- Cybersecurity Awareness Month

<https://staysafeonline.org/programs/cybersecurity-awareness-month/>

- Stay Safe Online Resources Library

<https://staysafeonline.org/resources/>

- Security Awareness Videos

<https://staysafeonline.org/resource/security-awareness-episodes/>

- CISA Cyber Essentials

<https://www.cisa.gov/cyber-essentials>

- #BeCyberSmart Campaign

<https://www.dhs.gov/be-cyber-smart/campaign>

NATIONAL CYBERSECURITY ALLIANCE

**OWN YOUR ROLE IN CYBERSECURITY:
START WITH THE BASICS**

Every individual should **own their role** in protecting their information and securing their systems and devices. There are many steps individuals can take to enhance their cybersecurity without requiring a significant investment or the help of an information security professional.

Below, NCSA highlights eight tips you can put into action now.

CYBERSECURITY BASICS:

- MAKE A LONG, UNIQUE PASSPHRASE**
Length trumps complexity. A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.
- PASSPHRASES AREN'T ENOUGH**
Use 2-factor authentication or multi-factor authentication (like biometrics, security keys or a unique, one-time code through an app on your mobile device) whenever offered.
- WHEN IN DOUBT, THROW IT OUT**
Links in email, tweets, texts, posts, social media messages and online advertising are the easiest way for cyber criminals to get your sensitive information. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. Essentially, just don't trust links.
- KEEP A CLEAN MACHINE**
Keep all software on internet connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware. Configure your devices to automatically update or to notify you when an update is available.

DEFINITION OF CYBERSECURITY:
Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack (Merriam-Webster)

staysafeonline STAYSAFEONLINE.ORG f staysafeonline

#BeCyberSmart
POWERED BY DHS

Cyber Lessons The Facts Common Scams Report an Incident The Campaign

» BeCyberSmart » The Campaign

BE CYBER SMART

Online safety can be here today and gone tomorrow when you overshare.



THANK YOU



RECOGNIZE & REPORT PHISHING

Do Your Part. [#BeCyberSmart](#)

