



Recognize & Report Phishing

Do Your Part. #BeCyberSmart



RECOGNIZE & REPORT PHISHING

Do Your Part. #BeCyberSmart





OCTOBER IS
CYBERSECURITY AWARENESS MONTH

#BeCyberSmart

STATE OF EMAIL SECURITY



FBI Reported:

- Phishing attacks were the **#1 CRIME TYPE IN 2022**
- Phishing attacks are responsible for **90% OF DATA BREACHES**



The IC3 Recorded:

- BEC resulted in adjusted **LOSSES EXCEEDING \$2.7 BILLION**

Gartner

Gartner:

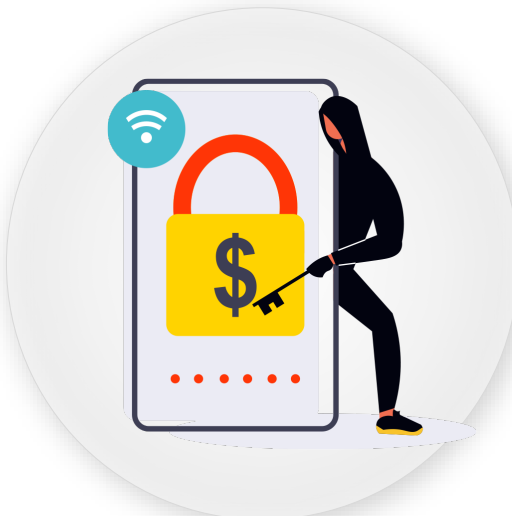
- **OVER 90% OF ORGANIZATIONS** have an awareness program, yet **69% OF EMPLOYEES** admit to intentionally bypassing company guidance
- **60% OF CYBERSECURITY TEAMS** spend **5% OR LESS OF THEIR BUDGET** on awareness activities
- **82% OF ALL BREACHES** involved **'THE HUMAN ELEMENT' IN 2022**



RECOGNIZE: What is Phishing?



URL



CREDENTIAL



ATTACHMENT

RECOGNIZE: Indicators of a Phish



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



1

From: christopher.mccoy@intlpackagedelivery.com

2

Subject: ATTENTION REQUIRED: TROUBLE WITH YOUR ORDER

3

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

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

4

[Order 3251351](#)

5

Enter your username password tracking number to verify the account.

All the best,
Christopher McCoy - Chief Support Manager.

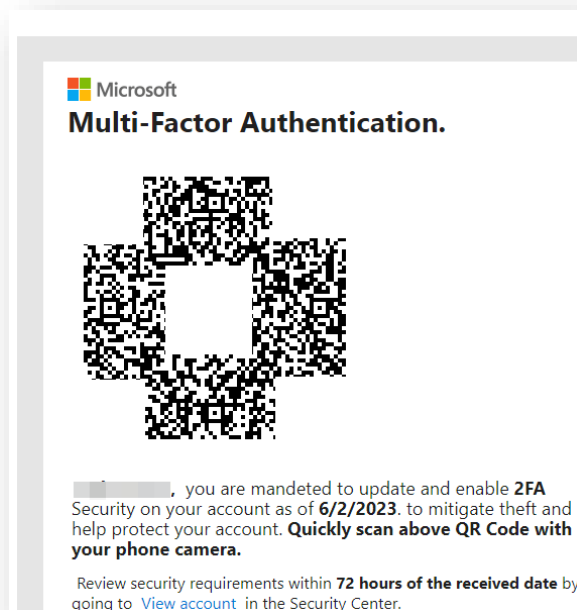
RECOGNIZE: QR Code Based Credential Phish



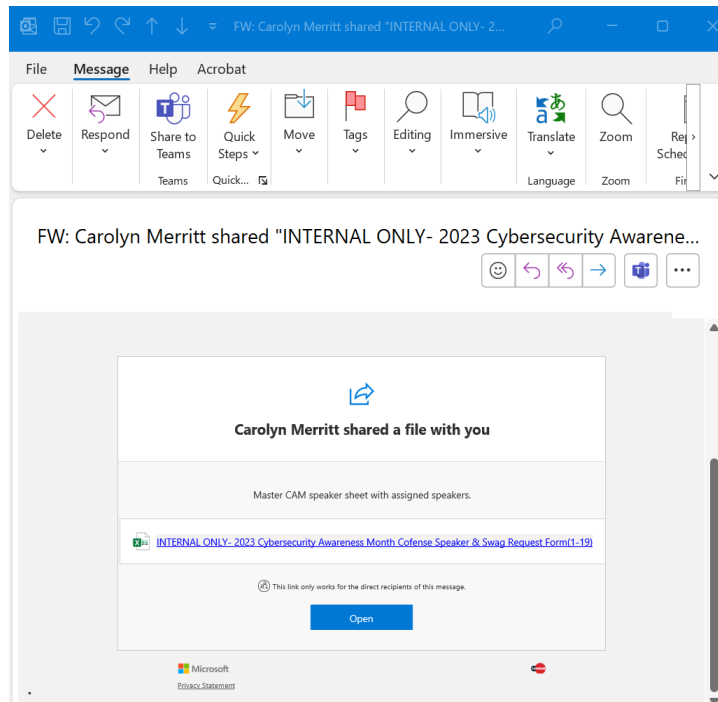
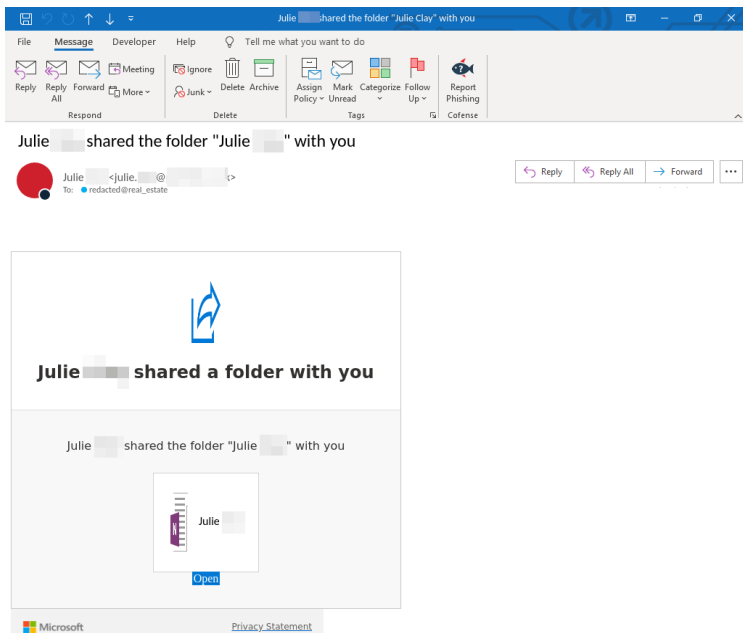
- **Spoofting Microsoft, or other, security notifications that ask a user to scan a QR code.**



- **Credential harvesting is not limited to Username and Password, it relates to any sensitive information you are asked to input.**



RECOGNIZE: Credential Phish via URL



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



RECOGNIZE: Credential Phish Landing Page



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

The screenshot shows a Microsoft login page overlaid on a background image of Rio de Janeiro. The page content includes:

- Microsoft logo and a back arrow.
- Section header: **Enter password**
- Warning text: **Because you're accessing sensitive info, you need to verify your password.**
- Input field: Password
- Checkbox: Keep me signed in
- Link: [Forgot password?](#)
- Button: **Sign in**



RECOGNIZE: Credential Phish via Attachment



Supplier Direct ACH/Wire Remittance

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

Supplier Direct ACH/Wire Remittance

REDACTED Payment Account-Team <info@[redacted].com>
To: redacted@insurance

.HTM
512 B

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

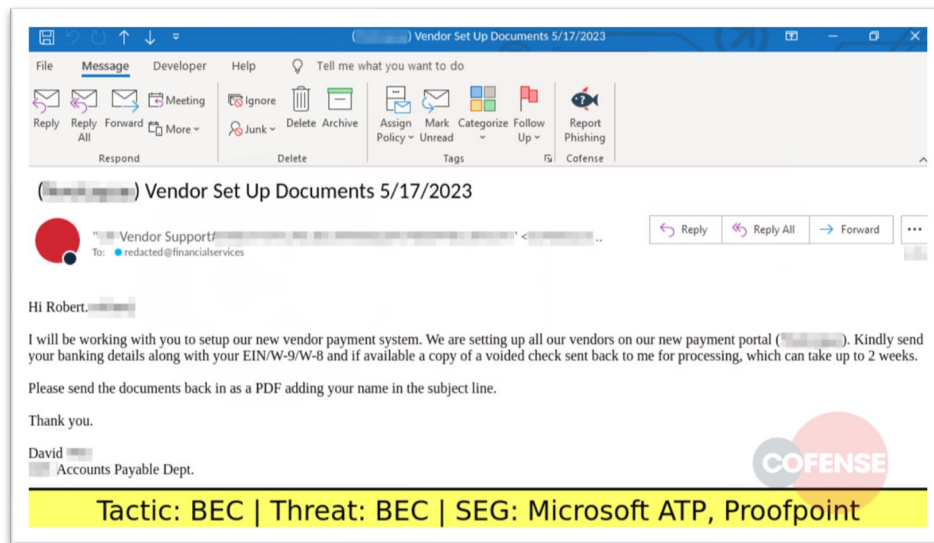
Tactic: HTM Attachment | Threat: Credential Phishing | SEG: Proofpoint



RECOGNIZE: Business Email Compromise (BEC)



1. Impersonate person of authority within the organization
2. Often request communication change to mobile device/SMS
3. Contains no URLs or attachments
4. Appeals to sense of urgency and authority
5. Often requires email reply for actual intent
6. Most common themes include:
 - Gift Card Requests
 - Direct Deposit Changes
 - Finance/Customer Data



RECOGNIZE: Business Email Compromise (BEC)



Always Observe Policy



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



**Always Check Reply-to
Addresses**



RECOGNIZE: BEC – Direct Deposit



The screenshot shows an Outlook email window titled "Direct Deposit Update". The ribbon includes "File", "Message", "Developer", and "Help". The "Message" ribbon has several groups of actions: "Respond" (Reply, Reply All, Forward, More), "Delete" (Ignore, Delete, Archive, Junk), "Tags" (Assign Policy, Mark Unread, Categorize, Follow Up), and "Cofense" (Report Phishing). The email content shows a sender "Russell" with a red profile picture, sending to "redacted@energy" on "Tue 05/30/2023". The body of the email says "Hi Sara," followed by a question about changing direct deposit information. A yellow banner at the bottom contains the text "Tactic: BEC | Threat: BEC | SEG: Microsoft ATP".

Direct Deposit Update

Russell <otta@.net>
To: redacted@energy

Tue 05/30/2023

Hi Sara,

I recently switched to a new financial institution and I do like to change my Paycheck Direct Deposit information, would the change be effective for the next pay date?

Thanks,
Russell

Tactic: BEC | Threat: BEC | SEG: Microsoft ATP




RECOGNIZE: BEC – Free?



The screenshot shows an Outlook email window with the title "Are you available". The ribbon includes "File", "Message", "Developer", and "Help". The "Message" ribbon is active, showing options like Reply, Reply All, Forward, Meeting, Ignore, Delete, Archive, Assign Policy, Mark Unread, Categorize, Follow Up, and Report Phishing. The email content is as follows:

Are you available

 James [redacted] <po[redacted]524@gmail.com>
To: ● redacted@medical

Thu 06/08/2023

↩ Reply ↩ Reply All → Forward ⋮

HI

Just let me know if you're free. I'm getting ready to give my loyal staff members some gifts. I need you to handle a brief task for me.

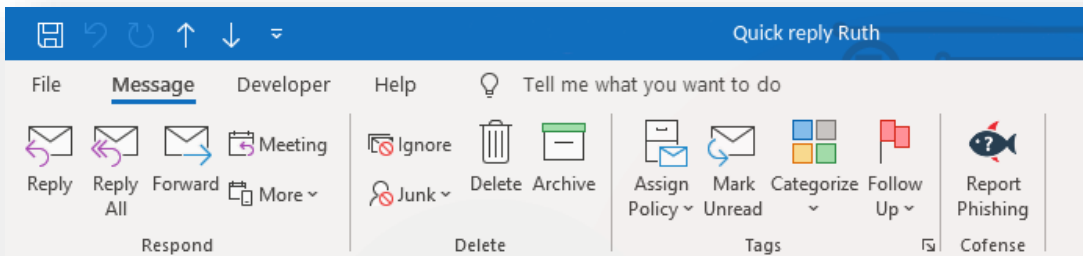
Regard
James [redacted]
Chief Executive Officer
sent it from a mobile device.

COFENSE

Tactic: BEC | Threat: BEC | SEG: Cisco Ironport



RECOGNIZE: BEC – Gift Card

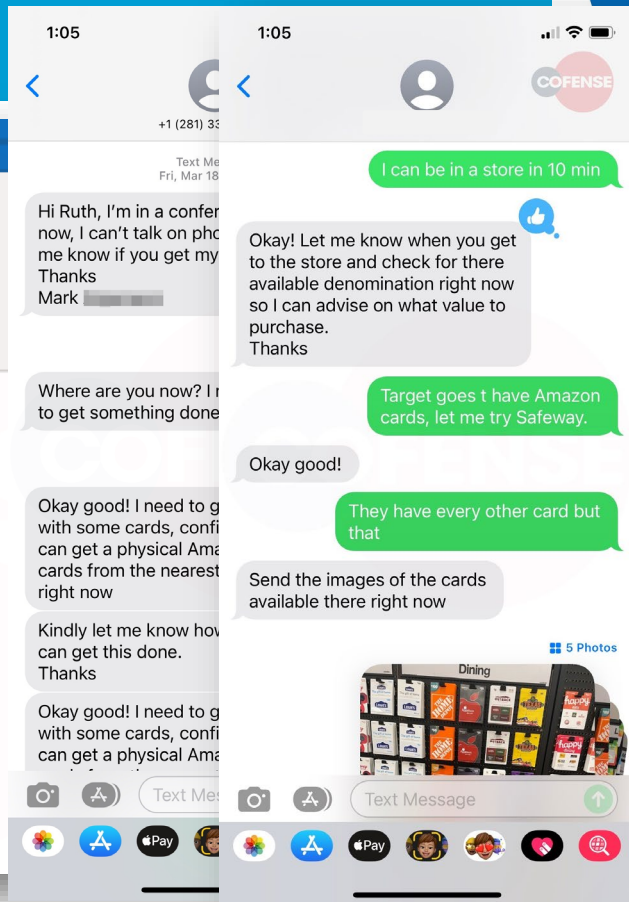


Quick reply Ruth



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

Mark [redacted].
Best Regards,



RECOGNIZE: Malware via Link



The screenshot shows an Outlook email window with the following details:

- Subject:** Re: [redacted] Invoices
- Sender:** [redacted]@[redacted].co.kr
- To:** [redacted]@real_estate
- Date:** Mon 05/01/2023
- Body:**

Hey There,

Please view the paperwork in the url down below.

[LINK](#)

Enjoy a good working day!

The interface includes a ribbon with 'Message' selected, showing options like Reply, Reply All, Forward, Meeting, Ignore, Junk, Delete, Archive, Assign Policy, Mark Unread, Categorize, Follow Up, and Report Phishing. A yellow banner at the bottom of the screenshot contains the text: **Tactic: Link | Threat: QakBot | SEG: Proofpoint**



RECOGNIZE: Smishing & Vishing

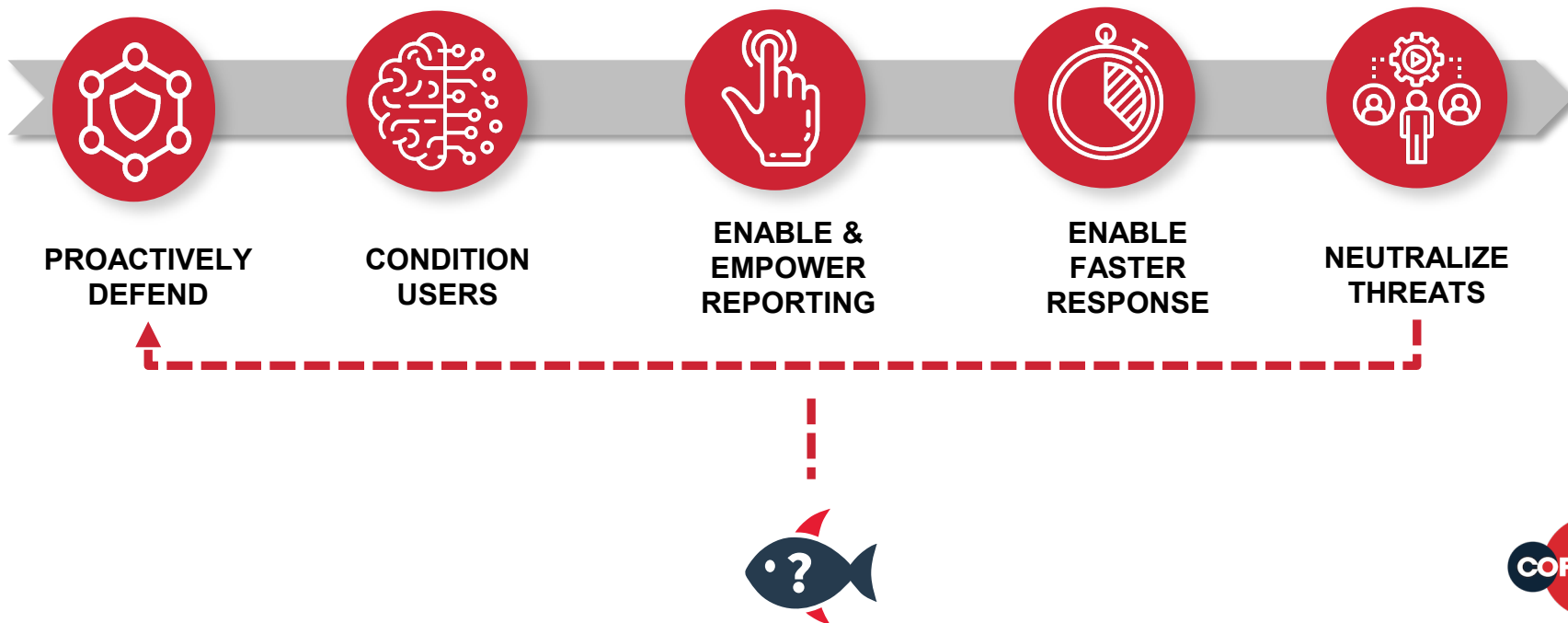


SMISHING

VISHING



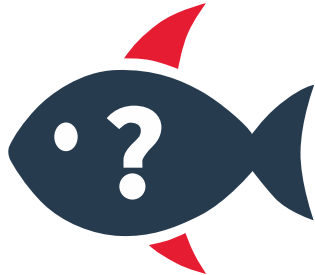
REPORT: Phishing Response Timeline



REPORT: What can we do?



Report the email



BE CYBER SMARTER: @HOME



Create Unique Accounts



Password Vault

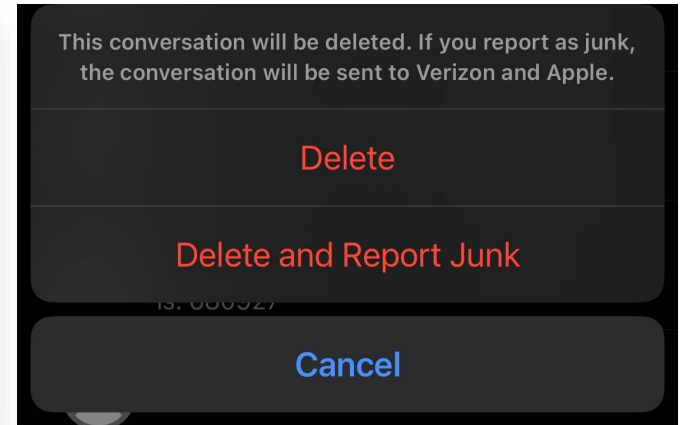
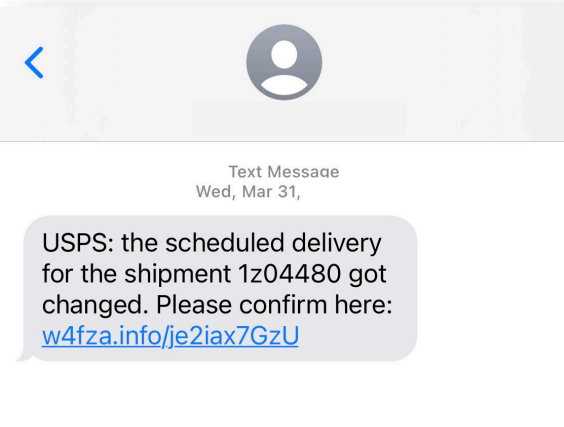


Enable 2FA

<https://2fa.directory>



BE CYBER SMARTER: @HOME



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

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

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 CYBER SECURITY 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 staysafeonline

#BE CYBER SMART
POWERED BY DHS

Cyber Lessons The Facts Common Scams Report an Incident The Campaign

BE CYBER SMART

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





CYBERSECURITY IS EVERYONE'S JOB. INCLUDING YOURS.

LEARN HOW EASY IT IS TO STAY SAFE ONLINE.

#BeCyberSmart



Thank you for downloading this Cofense guide. Carahsoft is the vendor, reseller, and OMG-Vendor for Cofense Cybersecurity solutions available via NJSBA, Texas DIR, MHEC, and other contract vehicles.

To learn how to take the next step toward acquiring Cofense's solutions, please check out the following resources and information:



For additional resources:
carah.io/CofenseResources



For additional Forward Networks solutions:
carah.io/CofenseSolutions



To purchase, check out the contract vehicles available for procurement:
carah.io/CofenseContracts



For upcoming events:
carah.io/CofenseEvents



For additional Cyber solutions:
carah.io/Cybersecurity



To set up a meeting:
Cofense@carahsoft.com (888)-662-2724