The Cyber Attack Landscape

Is Your Organization Prepared?

Presenters

Mike Lettman

Director of Security Operations

michaellettman@tcbk.com

Jason Levingston

SVP, Chief Information Officer

jasonlevingston@tcbk.com

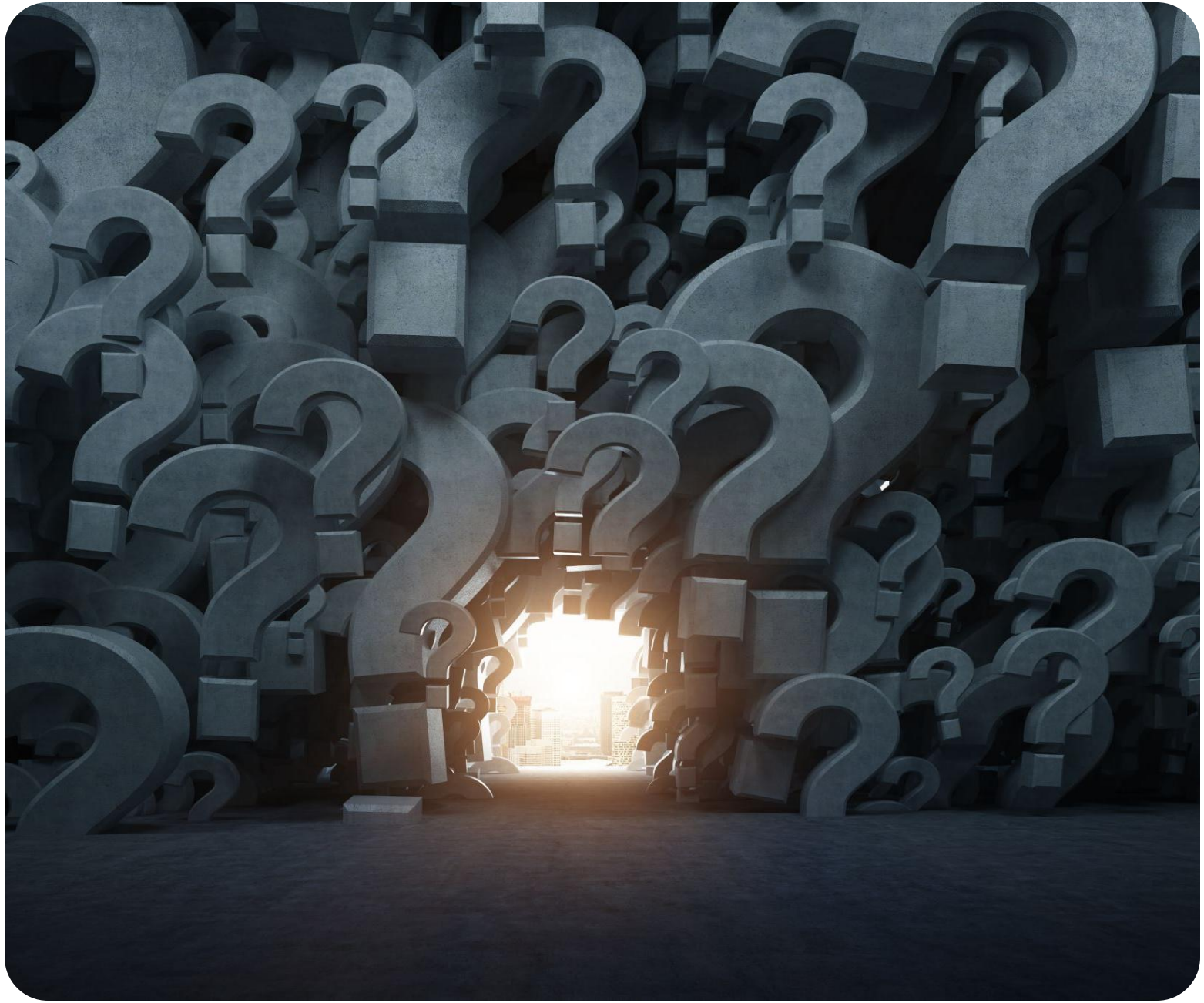
Paul Abramson

EVP, Chief Technology Officer

pabramson@arb.bank

Agenda

- Threat actors: who is targeting your organization and how
- Top of mind vulnerabilities and risks
- Key concerns around detection, response, and resilience
- Emerging defense strategies and technologies
- Relevant regulatory guidance
- Takeaways



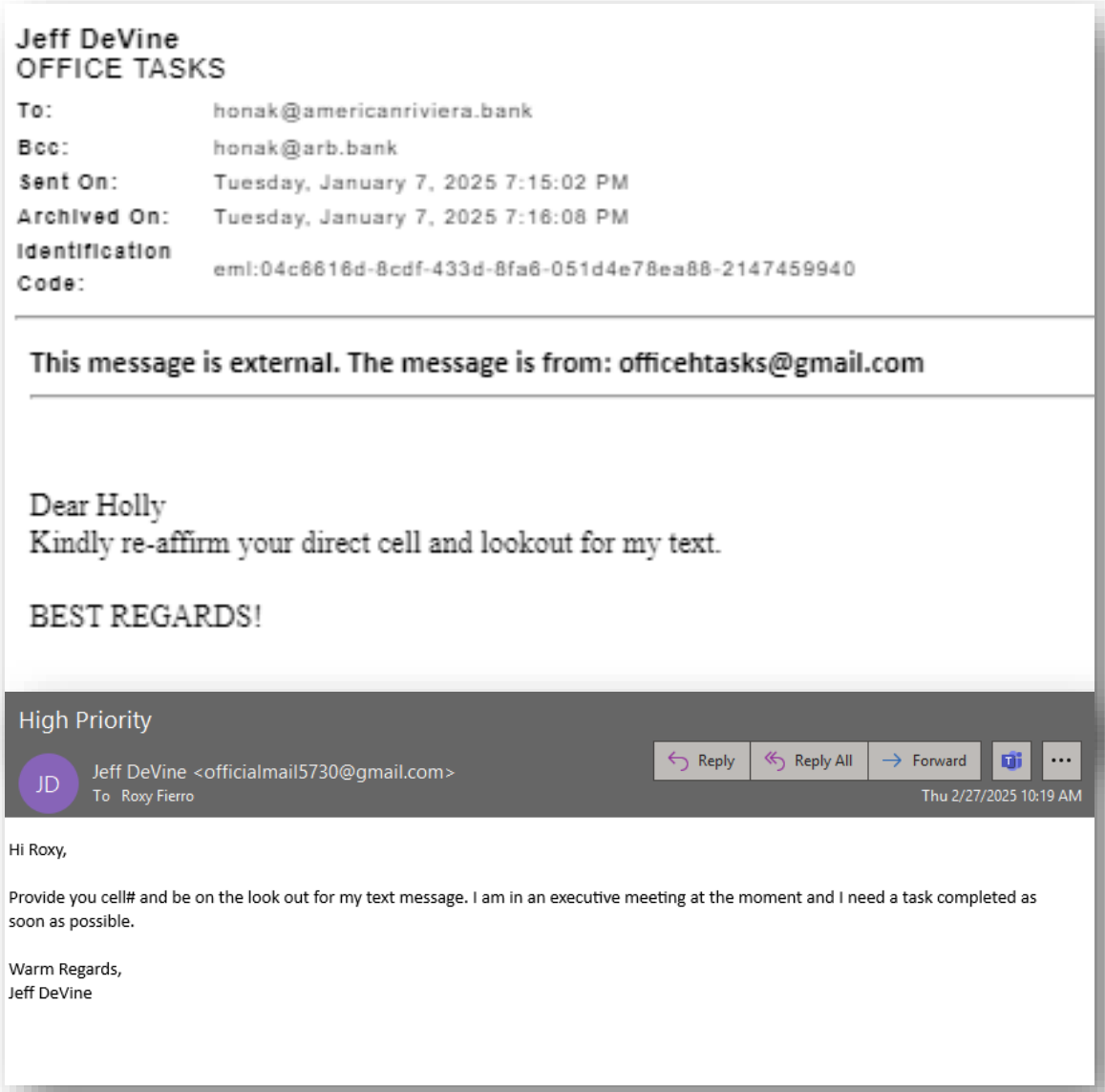
Top of Mind Risks

- Cyber Facts and Figures
- Scams/Theft
- Cloud Platform Security
- AI – Defensive Posture

Cybersecurity Facts and Figures (2025)

- 47% of organizations are concerned about adversarial advances powered by generative AI.
- 49% of public-sector organizations feel they lack the necessary talent for cybersecurity.
- 54% of large organizations cite supply chain challenges as the biggest barrier to achieving cyber resilience.
- 66% of organizations expect AI to significantly impact cybersecurity in the coming year, but only 37% have security assessment processes for AI tools.
- The skills gap in the cybersecurity workforce increased by 8% since 2024.
- 72% of organizations report an increase in cyber risks, with ransomware being a top concern.
- Fragmentation of cybersecurity regulations complicates compliance for organizations.

(Source: World Economic Forum)



Jeff DeVine
OFFICE TASKS

To: honak@americanriviera.bank
Bcc: honak@arb.bank
Sent On: Tuesday, January 7, 2025 7:15:02 PM
Archived On: Tuesday, January 7, 2025 7:16:08 PM
Identification Code: eml:04c6616d-8cdf-433d-8fa6-051d4e78ea88-2147459940

This message is external. The message is from: officehtasks@gmail.com

Dear Holly
Kindly re-affirm your direct cell and lookout for my text.

BEST REGARDS!

High Priority

JD Jeff DeVine <officialmail5730@gmail.com>
To Roxy Fierro

Reply | Reply All | Forward | ...

Thu 2/27/2025 10:19 AM

Hi Roxy,

Provide you cell# and be on the look out for my text message. I am in an executive meeting at the moment and I need a task completed as soon as possible.

Warm Regards,
Jeff DeVine

Scams/Theft

- Similar scams target both employees and customers
- Bank impersonations
- CEO impersonations
- Payroll scams both payroll funding and individual direct deposit
- Vendor invoice payments / change of payment info
- Targeted business impersonation through email

Payroll Theft Attempts

Hello Fernanda Hernandez,

I'm writing to request a change to my banking information on file. My previous bank account information is no longer valid, I would love the changes before the next payday. Thank you for your understanding and assistance in making this change. If you have any questions, please feel free to reach out to me.

Thanks,
Kylleen Wisham.
Fvp, Digital Banking Manager.

Hello Roxy,

I will need you to complete a task while I'm in an executive meeting, so please provide your phone number in your email response and await my text.

Best Regards.

Hi,

I switched banks recently and need your help updating my ACH/Direct deposit info on the system to my new bank account. My old account will be inactive soon.

Should I send you my new bank details now to make the change ?

Thanks.

UPDATE TO DIR. DEPOSIT DETAILS

HW Heather Watter
To Vanesa Wendler
2/20/2025

Hi Vanesa,

I trust you're doing well. Unfortunately, my previous account has been compromised and I'll like to update my Direct deposit info on file before next payroll is processed. Could you pls guide me through the process.

Best Regards
Heather Watters
Assistant Vice President, Marketing Officer at
American Riviera Bank (arbv)

Targeted Phishing Attempts

Scammers respond to previous email to bank employee

Register look-alike domains

Requests signature card via DocuSign

Request follows to enroll in online banking with access to wires and ACH

We have a new trustee and would like to add and enroll Kenneth to the signature card of all our accounts to have full admin and full transactional access.

Kindly email me required document/information needed to complete the enrolment.

Thanks,

Microsoft Direct Send Abuse

Attackers use direct send to bypass email security solutions

Connect directly to the Exchange Online server

Send to onmicrosoft.com email address

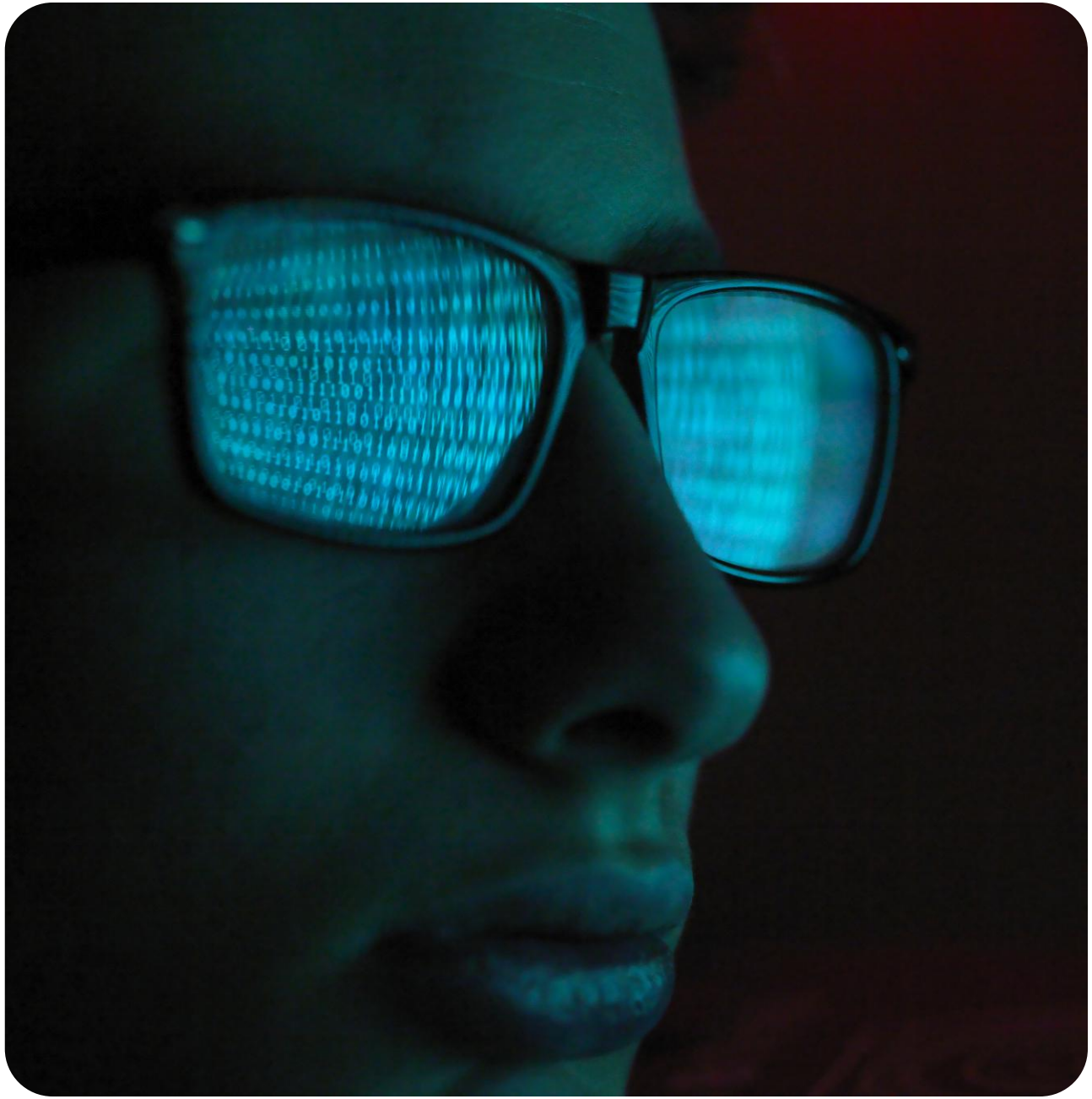
Allowed by default

What should banks do?

- Perform risk assessments
- Assess maturity
- Know your vendors,
- Defense in Depth
- Understand the environment and default security

Insider Threats

- Employee logging into a hosted third-party application with inconsistent security controls
- Ability to upload sensitive data to Gmail and other personal accounts
- Computer infected with ransomware creating a PR nightmare



Artificial Intelligence - Data Loss

- Access to uncontrolled AI tools
- Use of “public” interfaces to approved tools like Copilot
- PII vs. sensitive data
- Microsoft Enterprise Data Protection safeguards customer data against prompt injections, harmful content and copyright concerns.

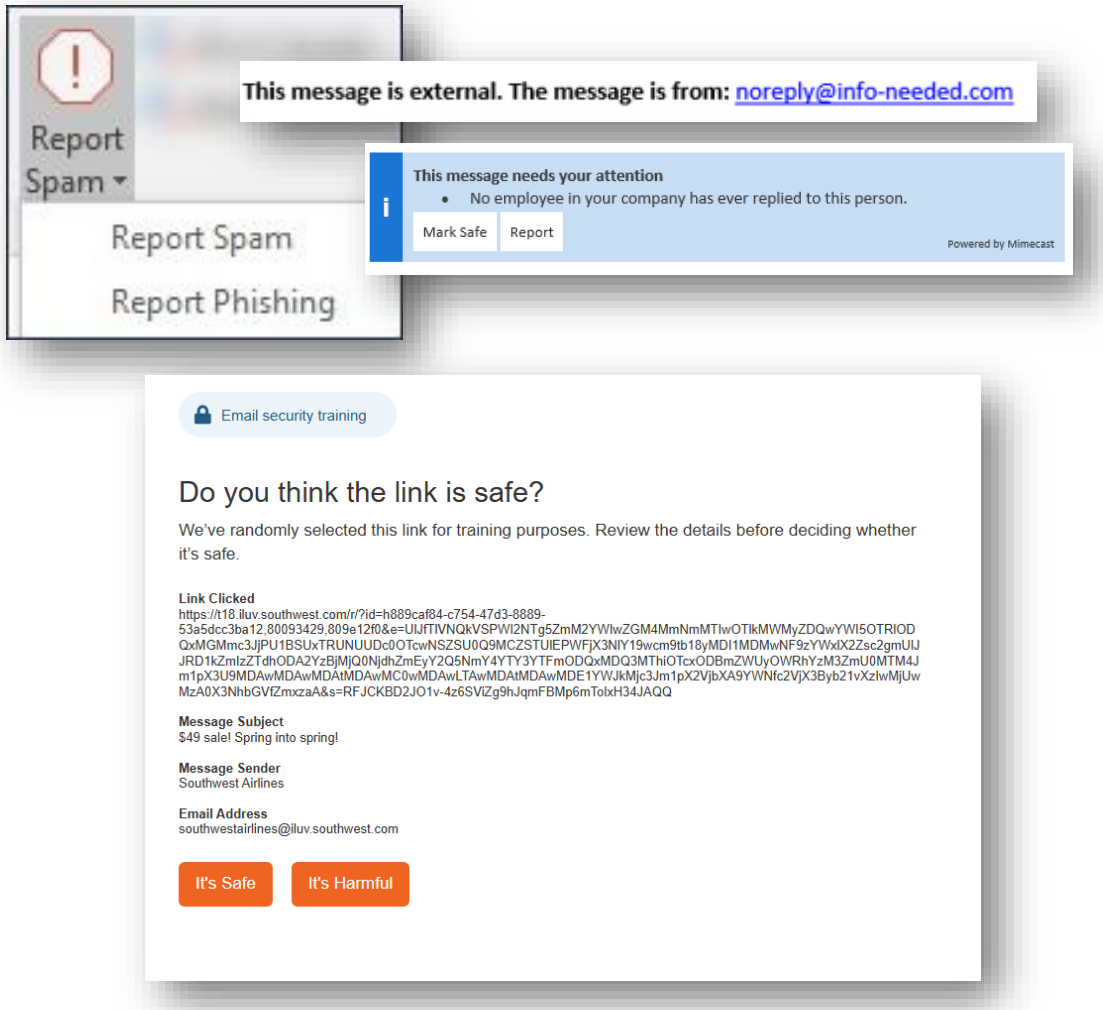
While banks leverage AI in business and for cybersecurity defenses, cyber criminals will exploit AI to develop more sophisticated attacks including deepfakes and automated malware.

```
# Bing
local-zone: "bing.com" redirect
local-data: "bing.com CNAME nochat.bing.com"
local-zone: "www.bing.com" redirect
local-data: "www.bing.com CNAME nochat.bing.com"

#CoPilot
local-zone: "copilot.microsoft.com" redirect
local-data: "copilot.microsoft.com CNAME cdp.copilot.microsoft.com"
```

Defense Strategies – Protect Systems, Data, and Customers

Recommendations for IT Teams

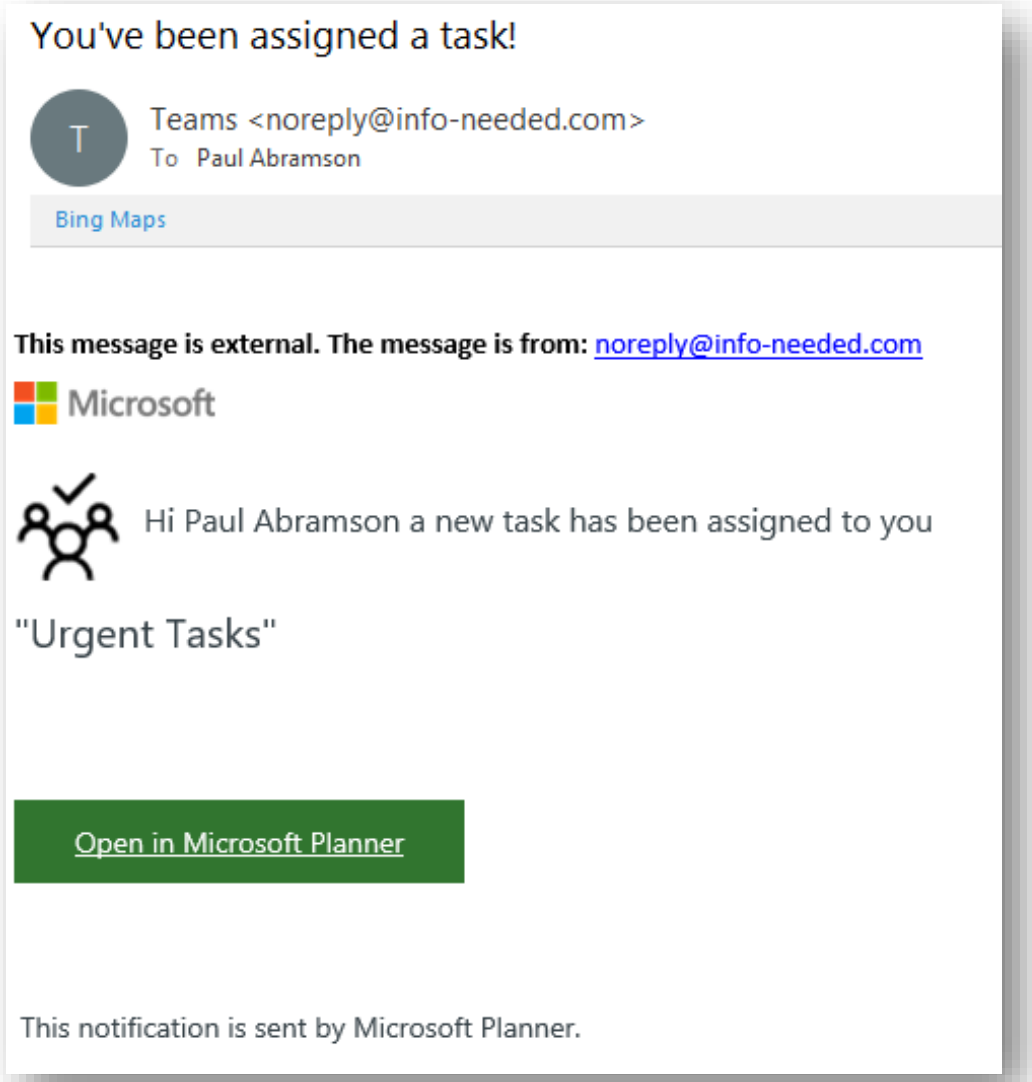


- Email Security (e.g., impersonation protection) - keep lists current: new hires are targeted within days of LinkedIn profile changes
- Audit cloud systems and close holes (e.g., Exchange direct send)
- Explore enhancements with existing vendors (e.g., email security URL protection and awareness modules)
- Enterprise browser technologies apply granular data loss, malware, and phishing protection
- Leverage SSO process through Identity providers (e.g., Entra ID, Okta, or others) to ensure consistent access control

Identity and Access Management / SSO

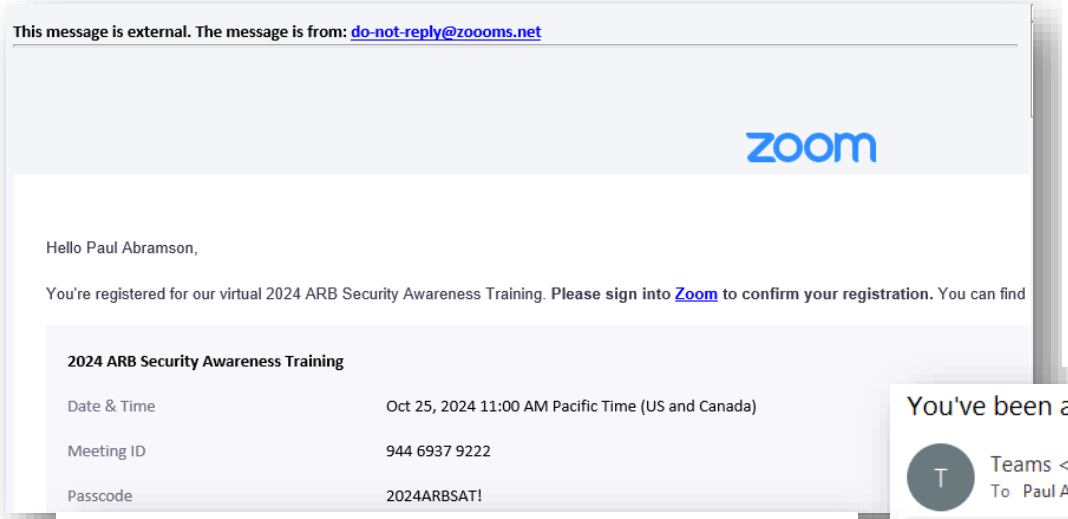
- Configuration policies to restrict access to cloud platforms
- Approval process to access other tenants
- Prevent unintended data sharing
- Leverage SSO where applicable to apply controls to other environments / third party providers (e.g., core, TPRM platforms, fraud tools, CRM, etc.)

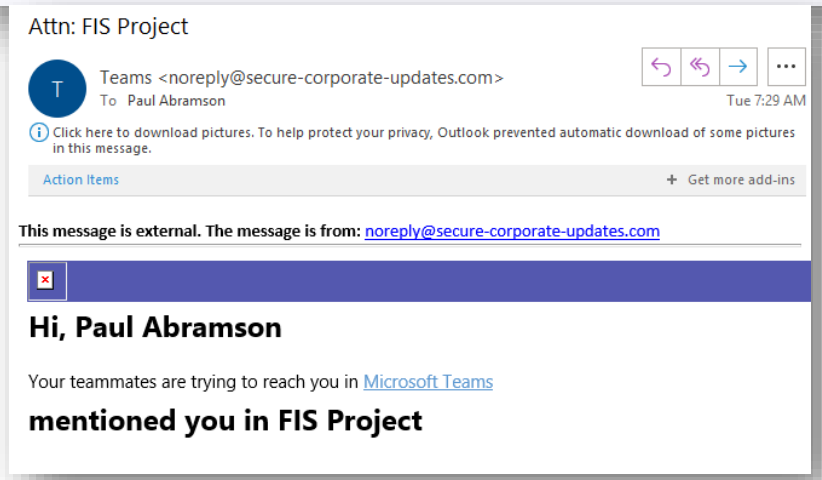
Phishing Tests and Awareness

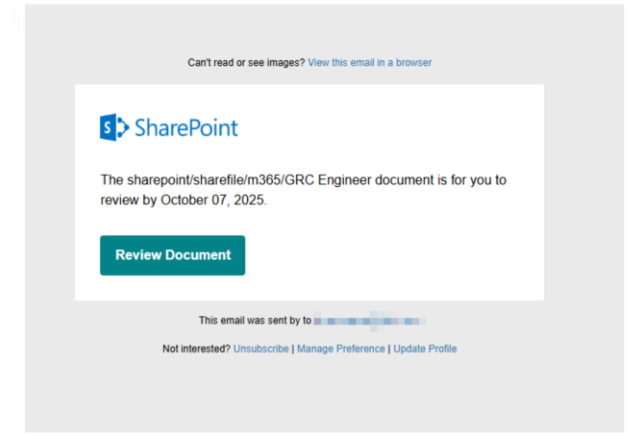


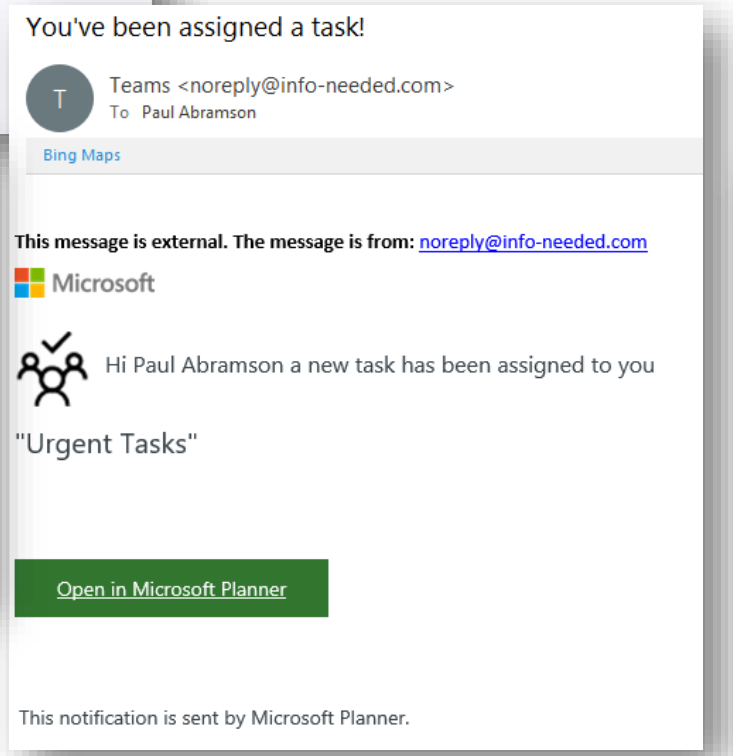
- Tough but fair testing
- Use known third parties like Microsoft, FIS, Fiserv, ABA, CBA, IRS, HR systems (threat actors are becoming more sophisticated… so should our testing)
- Targeted exercise based on business area
- Track results based on users who report as well as click/fail
- Consider instant notification to employee on individual test results (i.e., Congratulations! This was a phishing test…).
- Immediate training and escalation process

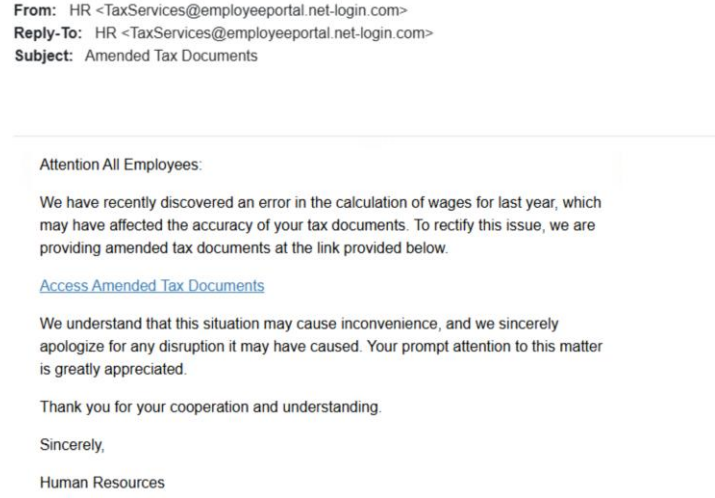
Internal Phishing Tests

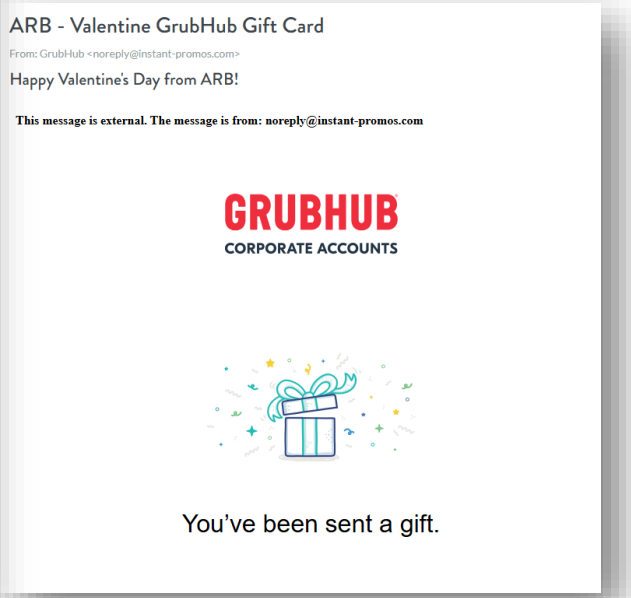












Regulatory Guidance for Cybersecurity

Examples of Reportable Notification Incidents
1. A large-scale distributed denial of service attack disrupts customer account access for an extended period (e.g., more than four hours).
2. A bank service provider that is used by a banking organization for its core banking platform to operate business applications is experiencing widespread system outages and recovery time is undeterminable.
3. A failed system upgrade or change results in widespread user outages for customers and employees.
4. An unrecoverable system failure results in activation of the business continuity or disaster recovery plan.
5. A computer hacking incident disables the bank's operations for an extended period.
6. Malware on a bank's network poses an imminent threat to its core business lines or requires a bank to disengage any compromised products or information systems that support the bank's core business lines from internet-based network connections.
7. A ransom malware attack encrypts a core banking system or the bank's backup data.

- GLBA Safeguards Rule
- New CCPA Cybersecurity Audit Requirements outside of the GLBA exemption
- Interagency Guidance on Response Programs and FDIC Guidance https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin06/siwinter06-article1.pdf
- California Breach Notification Requirements for unauthorized acquisition of computerized data
- GLBA Breach Notification Requirements for unauthorized access to or use of customer information
- Federal Regulator Breach Notification Rule for Reportable "Notification Incidents" no later than 36 hours
- Notice to Attorney General upon a breach affecting more than 500 California residents
- Ransomware Self-Assessment Requirements
- Cyber Risk Institute (CRI) Profile and maturity model assessment based on NIST CSF

Bankers Electronic Crimes Task Force

CSBS

Ransomware Self-Assessment Tool (R-SAT)

CYBER RISK INSTITUTE

Takeaways

- ❑ Review recommendations to address vulnerabilities with your IT team
- ❑ Consider conducting ransomware and/or data breach tabletop exercises
- ❑ Implement/enhance phishing tests
- ❑ Review cybersecurity insurance coverage
- ❑ Collect evidence of client awareness / training activities
- ❑ Review internal policies and procedures against regulatory guidance