Shall We Play A Game: Are You Prepared To Survive A Cyber Crisis?

J.P.Morgan | CHASE

Disclaimer

This information is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided is intended to help clients protect themselves from cyber fraud. It does not provide a comprehensive list of all types of cyber fraud activities and it does not identify all types of cybersecurity best practices. You, your company or organization are responsible for determining how to best protect against cyber fraud activities and for selecting the cybersecurity best practices that are most appropriate to your needs.

© 2023 JPMorgan Chase & Co. All Rights Reserved.

Ohio Government Finance Officers Association (GFOA)

Hilton Cleveland Downtown, Cleveland, OH | Wednesday, October 11, 2023

An Interactive Exercise For All Audiences In Cybersecurity & Fraud Readiness, Prevention, & Resiliency

Will Kerr

Senior Cyber Range Technical Lead | Attack Simulation | Cybersecurity and Technology Controls

Exercise – Overview

Cyber and Fraud Exercise

Primary Exercise Objectives

- Using scenario-based questions and live polling, we will:
  - Discuss the role of business leadership and staff to prevent and recover from Cyber and Fraud Attacks
  - Examine types of Cyber and Fraud scenarios, and Threat Actor Tactics
  - Discuss methods to identify Cyber and Fraud attacks, and what or what not to do

Timing, Participants & Key Focus Areas

- **Timing:** 60 minute facilitated interactive exercise
- **Participants:** Ohio Government and Finance Officers
- **Key Focus Areas:**
  - Threat Tactics and Detection
  - Best Practices and Controls
  - Readiness
  - Business Resiliency and Continuity of Operations

High-Level Structure

- **Module 1** – **How Threat Actors Operate:** Can you identify potentially fraudulent activity?
- **Module 2** – **Mitigation and Recovery:** How can I reduce the likelihood, severity, and duration of impact from a cyber event?
- **Module 3** – **Readiness and Prevention:** Do you know how you and your business unit should be prepared to prevent an attack?

Discussion Guidelines

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise, and should not allow these considerations to negatively impact their participation

During this exercise, the following guidelines will apply:

- Discussion will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements are expected
- Respond to the scenario using your knowledge of current plans, capabilities, and insights derived from your training/experience
- This exercise is an opportunity to discuss and present multiple options and possible solutions
- There is no hidden agenda or trick questions
- Do not fight the scenario

State of the World

Today is October 11, 2023

For this exercise, consider the state of operations within your business, institution or government entity with regard to actual cyber & fraud attempts encountered or observed in current events. Geopolitical tensions remain high emboldening criminal threat actors to take advantage of the climate and emerging tactics, techniques, and procedures (TTPs). Social Engineering remains the primary method for attackers to gain access, implement malware, and conduct fraud activities. Additionally, the continued use of remote work post-pandemic and greater use of mobile applications for business purposes has expanded the attack surface for threat actors.

Please, keep in mind the primary focus of today’s discussion is to learn how threat actors use common methods to attack and defraud, and how institutions and their staff can best identify, prevent, and respond to such attacks.

START OF EXERCISE (“STARTEX”)

MODULE 1:
How Threat Actors Operate

Module 1 - Inject 1

Wednesday, October 11, 2023 @ 8:00 AM EST:

- You and others on your team receive texts from IT Support requesting they complete a form to register their mobile device on the organization’s Wi-Fi network

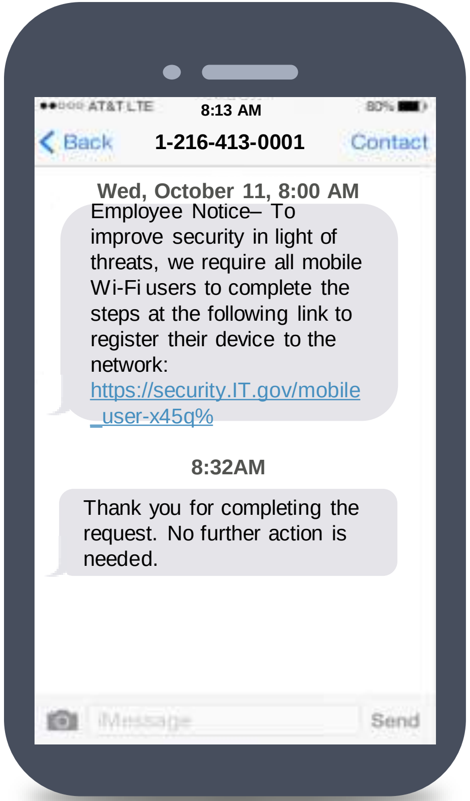
Based on the example, choose the appropriate action:

A. Click on the link and complete the requested steps

B. Forward to your managers and peers to make sure everyone has it

C. You think it’s suspicious, so you delete it

D. Report the text to IT support as suspicious



Wed, October 11, 8:00 AM

Employee Notice– To improve security in light of threats, we require all mobile Wi-Fi users to complete the steps at the following link to register their device to the network: https://security.IT.gov/mobile_user-x45q%

8:32AM

Thank you for completing the request. No further action is needed.

Module 1 - Inject 2

Thursday, October 12, 2023 @ 9:00 AM EST:

- A member of your team responded to the text from the previous day
- Upon clicking the link, the employee was directed to a webpage requesting they provide Name, Employee ID, Role, Email Address, and Mobile and Company Phone Numbers
- After completing the information, the form asks the user to download a “device ID Token” at a provided link
- The employee downloads the “token”

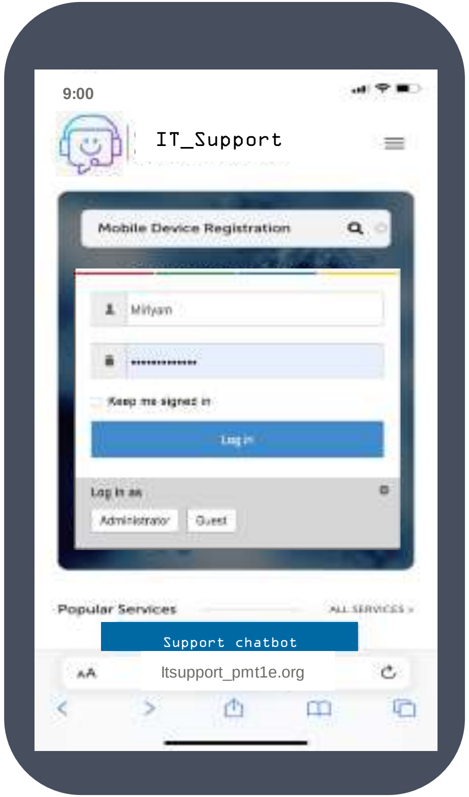
<u>Based on the example, what is the most likely result of the employee's actions:</u>

A. IT completes the process

B. Mobile device registration fails to work

C. Malware is downloaded to the mobile device

D. Both B & C



9:00

IT_Support

Mobile Device Registration

Mirlyam

•••••••••••••

□ Keep me signed in

J.P.Morgan | CHASE

Module 1 - Inject 3

Monday, October 16, 2023 @ 8:30 AM EST:

- Employees that completed the form and downloaded the token receive voicemails on their registered mobile device requesting the user return the call to resolve questions related to their mobile device registration. Several users return the call which are answered by representatives of the “Help Desk”
- The agent states there was an issue matching the provided name, ID and Username information with their profile in the system and ask the caller to validate the original information and provide their one-time password

Based on the example, choose the appropriate action:

A. User provides the one-time passcode and completes the process

B. The User asks the Help Desk representative to provide their employee ID to confirm their identity

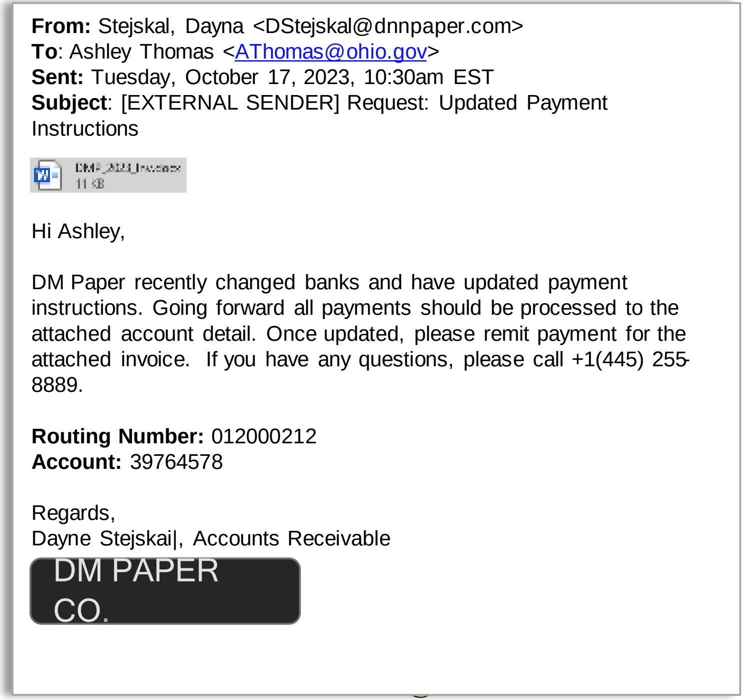
C. User believes the call is suspicious and ends the call

D. B or C

Module 1 - Inject 4

Tuesday, October 17, 2023 @ 10:30 AM EST:

- A member of the Accounts Payables department receives an email that appears to be from a known vendor stating that they are in the process of switching banks
- The sender provides updated bank account information to be used for payments
- The sender attaches an invoice for payment due



From: Stejskal, Dayna <DStejskal@dnnpaper.com>
To: Ashley Thomas <AThomas@ohio.gov>
Sent: Tuesday, October 17, 2023, 10:30am EST
Subject: [EXTERNAL SENDER] Request: Updated Payment Instructions

Hi Ashley,

DM Paper recently changed banks and have updated payment instructions. Going forward all payments should be processed to the attached account detail. Once updated, please remit payment for the attached invoice. If you have any questions, please call +1(445) 255-8889.

Routing Number: 012000212
Account: 39764578

Regards,
Dayne Stejskai|, Accounts Receivable

DM PAPER CO.

Based on the example, choose the appropriate action:

A. Update the payment information and pay the invoice as requested

B. Call Dayna at the phone number listed in the email to confirm

C. Contact the authorized agent using a documented callback procedure

MODULE 2:
Mitigation and Recovery

Module 2 - Inject 1

Friday, October 20, 2023 @ 10:30 AM EST:

- DM Paper Company contacts an accounts payable representative to inquire about a past due invoice
- The payables representative reviews their records and finds the payment had already been processed
- DM Paper states they did not receive any funds and verifies the account number to help locate the payment
- Further investigation finds that accounts payable sent the funds to a different account

Based on the example, choose the appropriate action:

A. Inquire with DM Paper as to why they sent new payment instructions and have them investigate the missing funds on their end

B. Contact law enforcement to report a fraud incident

C. Contact the bank holding your account to report a fraud incident

D. B and C

Module 2 - Inject 2

Monday, October 23, 2023 @ 8:15 AM EST:

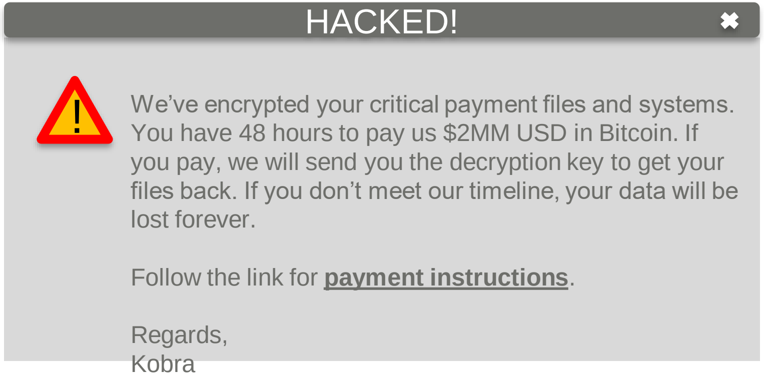
- Several employees in the accounts payable department are unable to log in to their payment application
- As more employees start their day, it becomes evident that nobody from accounts payable can log into the payment application
- Users open a ticket to IT Support
- Upon investigation, IT Support finds suspicious activity and engages their vendor for additional support
- The vendor finds a ransomware demand within the impacted file system

Based on the example, choose the appropriate action:

A. Contact law enforcement

B. Invoke the Accounts Payable Business Continuity plan and perform critical payments through the defined alternate process

C. Invoke the institutions crisis management process


HACKED! ✖

⚠ We’ve encrypted your critical payment files and systems. You have 48 hours to pay us $2MM USD in Bitcoin. If you pay, we will send you the decryption key to get your files back. If you don’t meet our timeline, your data will be lost forever.

Follow the link for **payment instructions**.

Regards,
Kobra

MODULE 3:
Readiness and Prevention

Module 3 - Inject 1

Monday, November 6, 2023 @ 10:00 AM EST:

- The organization completes their investigations into the root cause of the Business Email Compromise fraud and Ransomware attack
- It was found that a blended social engineering attack leveraging Smishing and Vishing allowed the threat actors to obtain credentials, deploy malware, and gain persistence within the network allowing for the interception of emails
- Leaders create Action Plans to resolve the issues and prevent similar attacks from being successful

Based on the example, choose the appropriate action(s):

A. Create recurring cyber and fraud training and testing programs

B. Establish crisis management plans with a defined maintenance process

C. Establish business continuity plans for critical business processes

D. All the above

Module 3 - Inject 2

Wednesday, November 8, 2023 @ 2:00 PM EST:

- The Accounts Payable team meets to discuss the Business Email Compromise (BEC) fraud and seek controls to minimize the risk
- Consulting industry best practices, the team discuss several options

Based on the example, which solutions minimize the risk of BEC fraud:

A. Establish a strong callback procedure to verify payment change requests

B. Review employee entitlements(access) to payment systems to right-size the number of users with privileged access

C. Implement daily account reconciliation

D. All the above

END OF EXERCISE (“ENDEX”)

Key Considerations for Payments Security

User Access

- Make sure you know who has access to your banking relationships and accounts; **review entitlements regularly**
- Set **payment limits** at account and employee level based on payment trends/history (e.g., 12-month history)
- Establish **multiple approval levels** based on various thresholds (e.g., dollar amounts, tenure)
- Ensure robust and multi-level approvals required in areas such as accounts payable
- **Don't have multiple users log in from the same computer** to initiate or release payments
- Use approved templates/verified bank lines and **restrict use of free form payments**

Reconciliation

- Perform **daily reconciliation** of all payments activity – Immediate identification and escalation is critical

Verification

- **Don't move money based solely on an email or telephone instruction(s),** even from trusted vendors
- **Validate by calling** the entity requesting payment/change in instructions at their known telephone number
  - Never call a number provided via an email or pop-up
- Always **validate the sender's email address** and hover over the email address and/or hit reply and carefully examine the characters in the email address to ensure they match the exact spelling of the company domain and the spelling of the individual's name
- Never give any information to an **unexpected or unknown caller**

Detection

- **Identify** irregularities (e.g., first time beneficiaries, cross-border payments)
- **Use multi-factor authentication (MFA)** wherever possible
- **Verify** payment values and velocity
- Establish **criteria** to verify or release payments
- **Track and trace** payments to detect modification

J.P.Morgan | CHASE

“Top 10 List” of Effective Programs/Practices

- Conduct an Independent Assessment
- Engage government and law enforcement
- Join an industry forum
- Simulate an internal attack
- Deploy mandatory employee training and testing
- Know your third party vendors
- Conduct Exercises & Drills
- Understand how money leaves your organization
- Implement controls for maximum effect
- Plan for Payment Contingencies

Q&A