



2026 NACHA Rule Updates and Fraud Monitoring Recommendations



March 24, 2026

Today's Topics

- 2026 NACHA Operating Rule Changes
- Fraud Awareness
- Fraud Monitoring Recommendations
- Employee Training Recommendations to prevent Phishing
- Operational Tools to Reduce Fraud Risk

Meet the Presenters



**Ed Skou,
Director of Treasury
Management**



**Rolin "Bud" Peets, CISSP | CIPM
Chief Protection Architect,
Harbor IT**



**John D. Flory III, Cyber
Security Practice Lead,
Harbor IT**

2026 NACHA Operating Rule Changes



Fraud Monitoring by Originators, TPSPs, and ODFIs

Risk-Based Monitoring Requirements

Originators, Third-Party Service Providers (TPSPs), and ODFIs must implement risk-based processes to detect unauthorized entries.

Annual Review: These processes must be reviewed each year to align with emerging risks.

Standard Company Entry Descriptions

Payroll and E-Commerce Descriptions: Establishes standardized descriptions for payroll (“PAYROLL”).

Fraud Monitoring as an ACH Originator effective June 19, 2026



ACH Originators should implement risk-based procedures to identify transactions that may be unauthorized. At a minimum, they should address the following areas:

- **Unauthorized Payments**

- Safeguard online banking credentials, which can be compromised through malware.
- Maintain separate email accounts for work and personal use.
- Avoid clicking on links until verifying legitimacy directly through a known phone number or the vendor's official website.

- **Authorized Payments Made Under False Pretenses**

- Independently confirm any vendor-related account changes or payment instructions by calling a trusted phone number, as email compromises and impersonation attempts can make fraudulent requests appear authentic.

Fraud Awareness

The Fraud Triangle

Why Fraud Happens

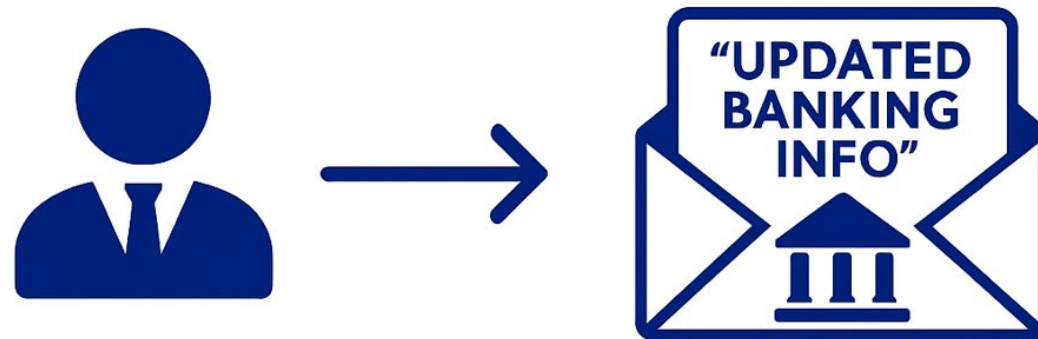


When These Overlap, **Fraud Risk Increases**

Five Common Fraud Tactics

1. Business Email Compromise (BEC) & Payroll/Vendor Impersonation

Impersonation of trusted parties to request payments or bank-detail changes



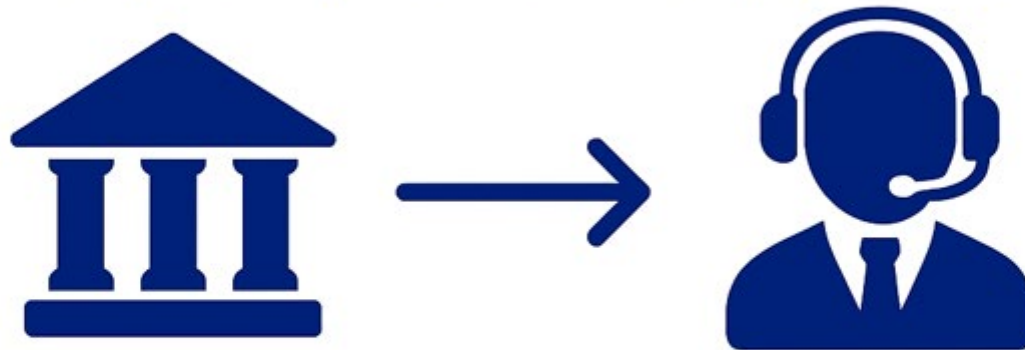
Fraudsters attempt to redirect payroll or vendor payments to fraudulent accounts.

- **Red flags:** Urgent requests, spoofed domains, off-hours messages; “updated banking info,” slight name/email variations
- **Control:** Callback verification of all payment-detail changes + dual control for payee edits

Five Common Fraud Tactics

2. Bank Impersonations

Fraudsters impersonate the bank, IT support, or Fraud department to trick clients into providing credentials, moving funds, verify ACH & Wire payments

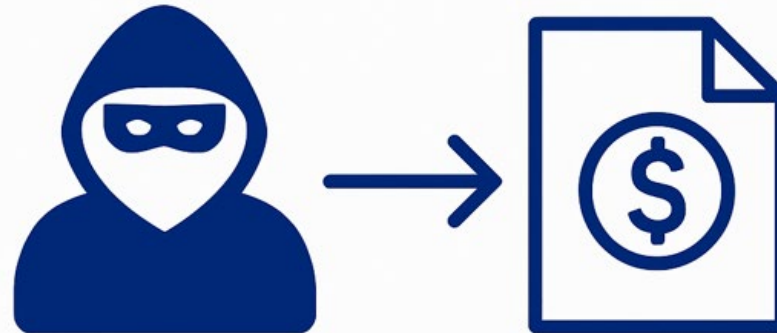


- **Red flags:** Requests to “verify” account numbers, login credentials, tokens, or ACH/Wire instructions
- **Control:** Never share credentials; verify bank-related calls using a known, trusted phone number

Five Common Fraud Tactics

3. Account Takeover (CATO)

Criminals use stolen credentials to originate unauthorized ACH transactions.

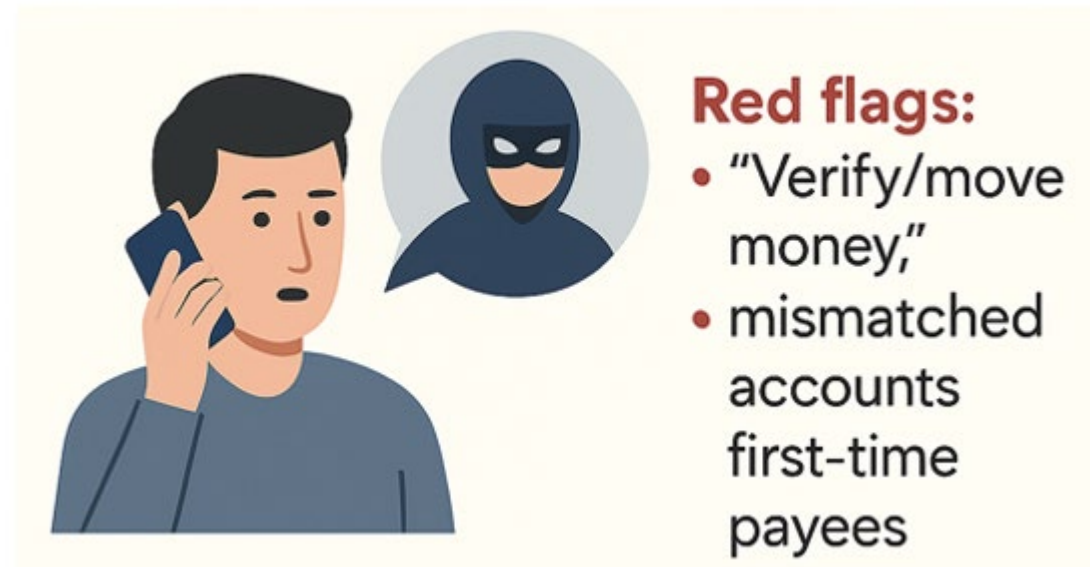


- **Red flags:** New templates, unusual timing or velocity.
- **Control:** Strong MFA + daily monitoring + Training

Five Common Fraud Tactics

4. Credit-Push Fraud (False Pretenses)

Victims are coached into authorized transfers under deception.



Control: Anomaly Monitoring + Employee/Social Engineering Awareness

Five Common Fraud Tactics

5. Fake Invoices / Purchase Order Scams

Fraudulent invoices that look legitimate but direct funds to criminals.



Red flags:

- Slightly altered vendor names, new routing numbers.

Control:

Independent invoice validation + segregation of duties.

Seven Controls for Preventing and Detecting Corporate Account Takeover



Seven Controls for Preventing and Detecting Corporate Account Takeover



Implement Segregation of Duties: Ensure that payment initiation and payment approval are performed by separate authorized users to reduce the risk of unauthorized transactions.

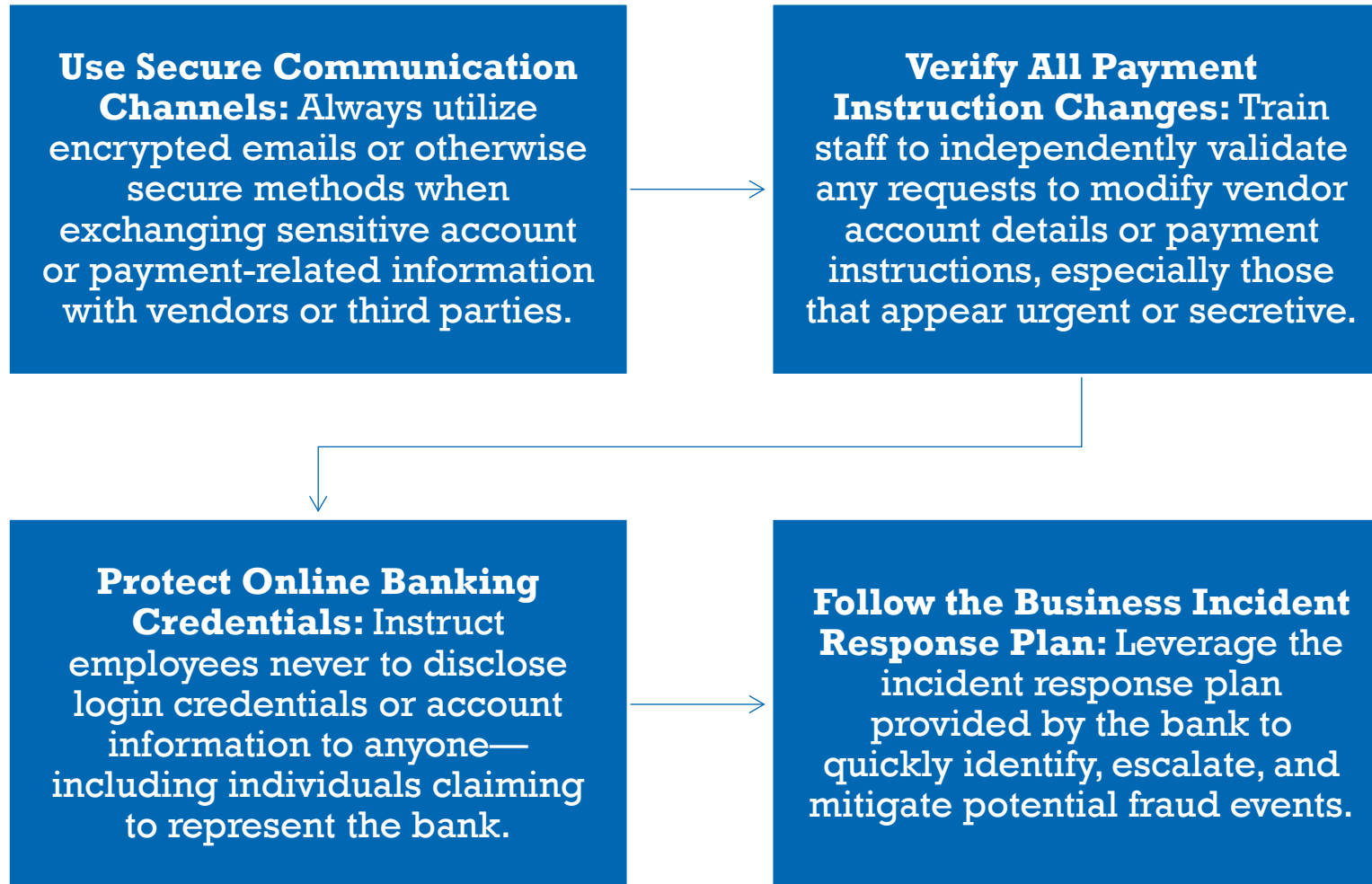


Conduct Daily Account Monitoring: Review account activity every business day and immediately contact the bank if any unusual, unexpected, or suspicious transactions are identified.



Provide Continuous Employee Awareness Training: Educate employees on how to recognize potential fraud attempts through email, phone calls, text messages, faxes, and mailed correspondence.

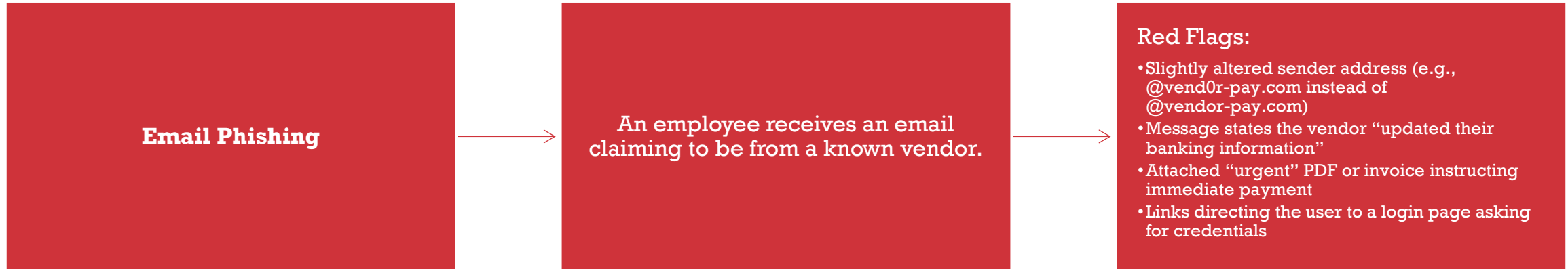
Seven Controls for Preventing and Detecting Corporate Account Takeover



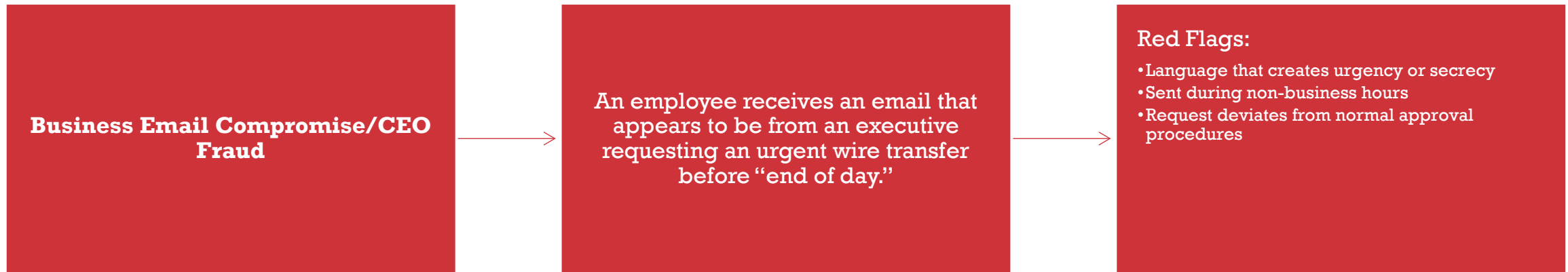
Employee Training Recommendations to Prevent Phishing



Train Your Employees to be Alert for Phishing Attempts



“See Something.....Say Something”



Be Alert, Aware and Prepared....Don't be a Victim

Four Common Phishing Attempts

1. Text Message (SMS) Phishing (Smishing)

A staff member receives a text claiming their online banking token is “locked” and they must click a link to reset it.



TEXT MESSAGE (SMS) PHISHING (SMISHING)

MESSAGE

Security: Your online banking token is locked, Reset here: bit.ly/reset

Red Flags:

- Unexpected security alert
- Shortened URL (e.g., bit.ly)
- Requests credential verification

DO NOT CLICK

Four Common Phishing Attempts

2. Phone-Based Social Engineering (Vishing)

A caller claims to be from IT support or the bank's fraud department.



PHONE-BASED SOCIAL ENGINEERING (VISHING)

A caller claims to be from IT support or the bank's fraud department.



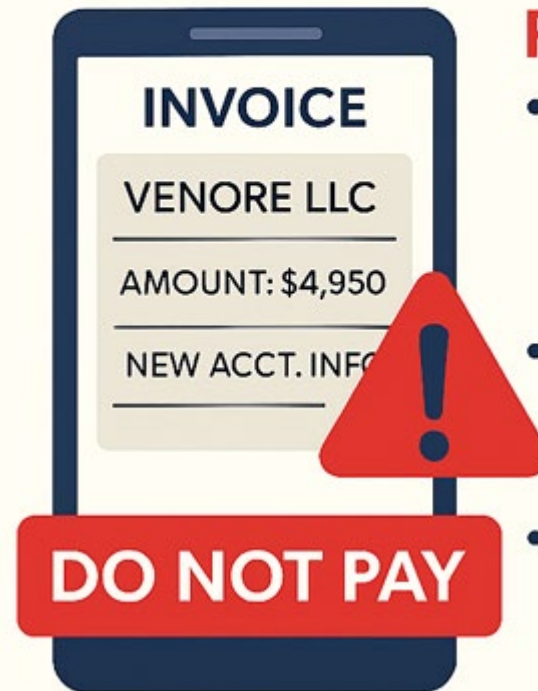
Red Flags:

- Caller pressures employee to "confirm login information"
- Claims of suspicious activity that require immediate action
- Caller ID spoofing matching the bank's number

Four Common Phishing Attempts

3. Fake Invoice or Purchase Order Scam

Accounts Payable receives an invoice for services that were never authorized or performed.

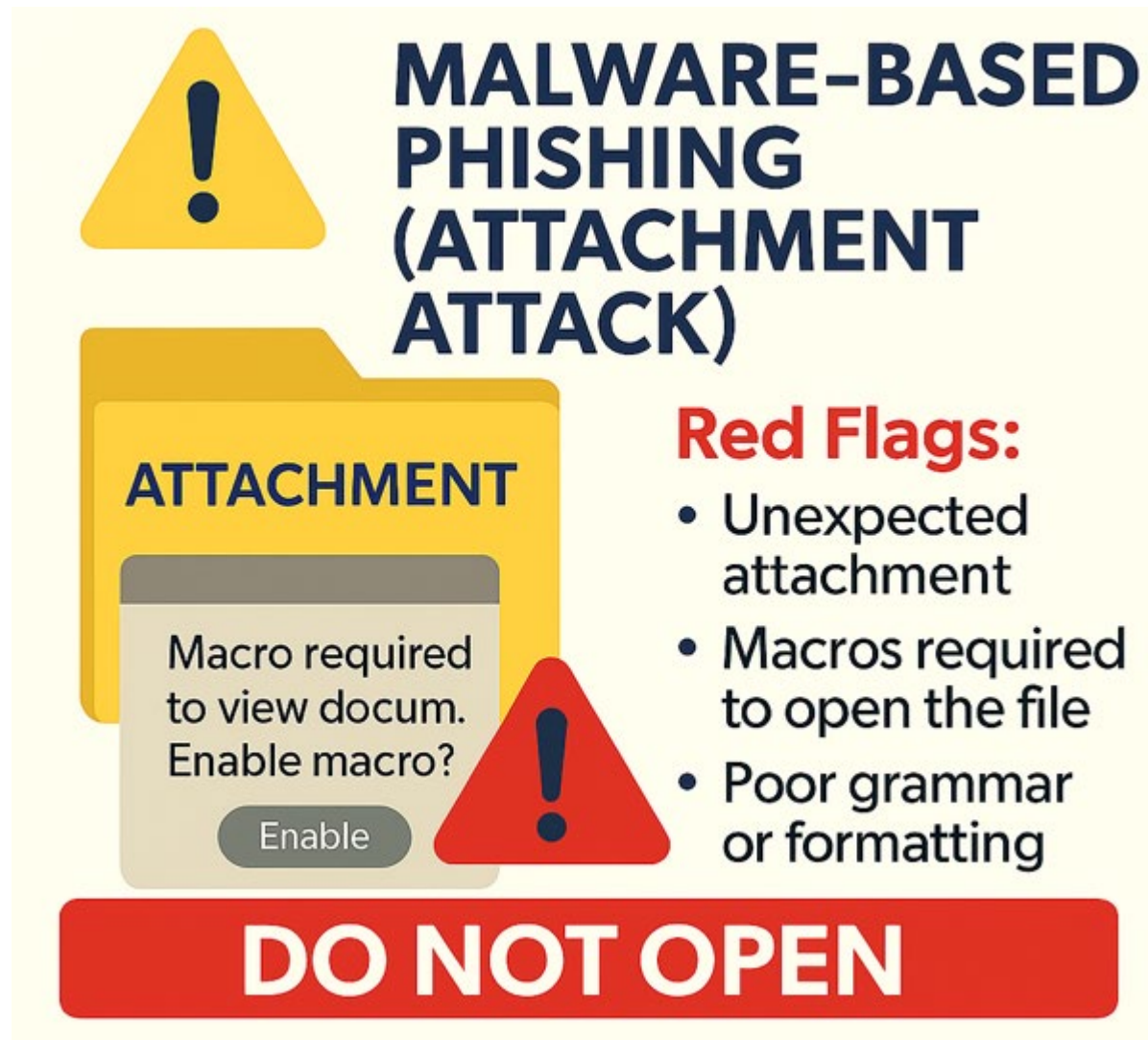


Red Flags:

- Vendor name resembles a real vendor but is slightly different
- New banking instructions included on the invoice
- Invoice amount slightly under approval threshold

Four Common Phishing Attempts

4. Malware-Based Phishing (Attachment Attack)



The infographic features a yellow background. At the top left is a yellow warning triangle with a black exclamation mark. To its right, the title 'MALWARE-BASED PHISHING (ATTACHMENT ATTACK)' is written in large, bold, dark blue letters. Below the title is a yellow folder icon labeled 'ATTACHMENT'. Inside the folder is a document icon with the text 'Macro required to view docum. Enable macro?' and a grey 'Enable' button. A red warning triangle with a black exclamation mark is positioned over the bottom right of the document icon. To the right of the folder, the text 'Red Flags:' is written in bold red, followed by a bulleted list of three items: 'Unexpected attachment', 'Macros required to open the file', and 'Poor grammar or formatting'. At the bottom of the infographic is a red banner with the text 'DO NOT OPEN' in white, bold, uppercase letters.

MALWARE-BASED PHISHING (ATTACHMENT ATTACK)

ATTACHMENT

Macro required to view docum.
Enable macro?

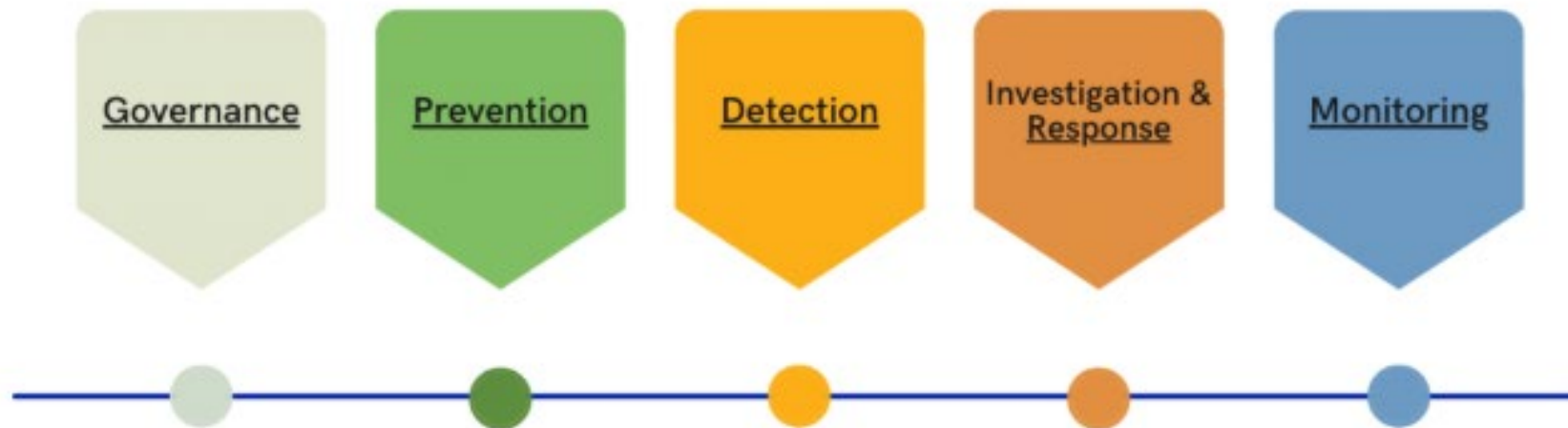
Enable

Red Flags:

- Unexpected attachment
- Macros required to open the file
- Poor grammar or formatting

DO NOT OPEN

Tools to Reduce Fraud Risk



Cybersecurity Insurance: A Financial Safety Net for Business



Offsets direct financial losses resulting from fraudulent activity.

Funds comprehensive forensic investigations and legal counsel.

Reimburses expenses for customer notification and identity monitoring.

Mitigates the impact of regulatory fines and penalties.

Facilitates rapid business recovery to minimize operational downtime.

Operational Tools to Reduce Fraud Risk



ACH & Check Positive Pay – Enables monitoring of check payments and ACH debits, allowing inappropriate or suspicious items to be identified and returned when necessary.

Secure Email to Vendors – Using password-protected, secure email reduces the risk of unauthorized access to sensitive documents, when possible.

RSA Token at Login – Adds an extra authentication layer, reducing the likelihood of unauthorized access. Users must have both their RSA token and personal PIN.

Dual Control for Payment Processing – Separating the roles of payment initiator and approver significantly lowers risk if a user's credentials become compromised.

Online Banking Alerts – Immediate alerts help ensure that most payments can be reversed when the bank is notified promptly.

Additional Resources

For additional fraud-prevention tools, educational resources, and up-to-date best practices, visit:

<https://www.southshorebank.com/webinarrecap>

[southshorebank.com/resources](https://www.southshorebank.com/resources)

nacha.org/rules/risk-management-topics-fraud-monitoring-phase-2

Contact Information

Treasury Service Team
BOB@southshorebank.com
781.682.3240

Ed Skou - Directory of Treasury Services
eskou@southshorebank.com

Harbor IT Contact

John D. Flory III – Cyber Security Practice Lead/vCISO
• John.flory@harborit.com
Rolin Peets – Chief Protection Architect
• rolin.peets@harborit.com



Questions