CORPORATE & INSTITUTIONAL BANKING

# CYBER SECURITY

## RESOURCE GUIDE

PNC SECURITY AWARENESS

PNC

# AWARENESS OF CYBER THREATS FOR PAYMENTS FRAUD

Payments fraud attempts are widespread across all industry types as a result of email compromises and financial malware infections. Understanding how these fraud schemes are designed to infiltrate/compromise your business and taking action to prevent them are critical to your defensive strategy.

It is imperative that employees with access to funds movement services are aware of these fraud schemes and can recognize potentially fraudulent or malicious activity against their email or PINACLE® login credentials. These are very real threats, and we encourage you to educate staff throughout your organization.

# ATTEMPTED PAYMENTS FRAUD VIA EMAIL COMPROMISE

Cybercriminals initiate fraudulent payment requests, or requests to change payment instructions, from email accounts that appear to be from a company executive (such as the CEO or CFO) or from a known external associate, such as a supplier. The fraudulent "From" email address may be a fictitious account in the executive's name, or it may be a slight variation of a legitimate supplier email address, both of which can trick the recipient into believing that the communication is valid. It is also possible that the sender's legitimate email account has been compromised, making it essential that employees are able to recognize the characteristics of a fraudulent payment request.

Also be mindful that even when an email account is not compromised, there is quite a lot of information available in "Open Source" records (social media, public records) that cyber criminals can obtain easily in developing such schemes. For example, large construction contracts, such as for universities or hospitals, are disclosed in public filings. Cyber criminals can access these records, register a website impersonating the legitimate contractor, and initiate communication with the university or hospital introducing a "new" accounts receivable contact and account number set up specifically for that contract. Often, the cyber criminals will wait several months before initiating contact and use open source records to identify accounts payable personnel.

In such schemes, the cyber criminals don't need to know the amount of the upcoming payment or even the projected date for the payment. Instructions sent typically state that "All payments going forward should be made to the new account number and to the attention of the new accounts receivable contact." As construction contracts are typically paid in net 30-, 60- or 90-day increments, often the victims are unaware of the fraud until weeks or months have passed, making recovery of funds extremely difficult. These types of schemes often involve losses in excess of $1 million.

Another email impersonation fraud scam targets employee direct deposits. Hacked or spoofed employee email accounts are used to request changes to the employee's direct deposit information. As with all email requests relative to payments, you should confirm them with the requestor at a known telephone number.

PNC

## RECOGNIZE THE TYPICAL EMAIL FRAUD REQUEST SCENARIOS

▶ A supplier requests changes to payment instructions for an upcoming payment.

▶ An email appears to be from a company executive to initiate an urgent payment — typically for an acquisition, investment, payment or some other confidential reason.

▶ An email appears to be from a company executive delegating authority to an attorney or other external party for the purpose of providing payment instructions.

## ⚠ RECOGNIZE THE WARNING SIGNS OF AN EMAIL COMPROMISE

▶ Fraudulent emails will typically request that the recipient take one or more of the following actions:
- Bypass established payment initiation and approval procedures.
- Keep the payment confidential.
- Provide immediate confirmation (to requestor) when the payment is executed.
- Communicate with the requestor only via email.

▶ The requests will often warn of serious repercussions for failure to comply.

▶ Many times the executive appearing to be requesting the payment is out of the office or unavailable (which the fraudsters have previously determined).

▶ The request varies from the typical payment pattern for the company or the sender.

▶ The recipient should ask:
- Does the CEO (or other executive) routinely communicate payment requests via email?
- Is the request consistent with other emails from the sender?
- Are the email signature and tone consistent with other emails from the sender?

## 🛡 TAKE ACTION TO HELP PROTECT AGAINST THIS THREAT

▶ Train your employees to be vigilant when reviewing and confirming payment requests, especially those conveying a sense of urgency and/or insisting on secrecy.

▶ Establish formal policies, procedures and controls for all payment initiation requests and additions/changes to your accounts payable (A/P) system.
- Executive management should communicate and follow the policies and procedures.
- Employees should be trained and empowered to recognize requests that deviate from the established procedures and obtain confirmation of such requests from the requestor in person or via a known telephone number.

◈ PNC

# DANGEROUS FINANCIAL MALWARE INFECTIONS

Phishing emails, often with generic subject lines such as "Invoice" or "Resume," can contain dangerous financial malware variants in attachments or links.

Once the malware has been installed on a computer, it redirects a user's online banking sessions to a malicious site that harvests access credentials, such as User ID, Operator ID, Password, Security Question responses and Token.

It is important to know that **financial malware is often not detected by antivirus software**.

## ⚠ RECOGNIZE THE WARNING SIGNS OF A MALWARE INFECTION WHEN USING PINACLE

- A malware infection may cause an operator to be:

  ▸ Unable to log in due to screens that delay or redirect the typical login experience

  ▸ Prompted to provide their token passcode or security question responses repeatedly or presented with a "System Unavailable" message during the login process

  **PINACLE will never prompt an operator to enter login credentials (including a token passcode or security question responses) multiple times during the login process.**

  ▸ Instructed to have another operator log in from the same computer as part of a security process or to reactivate/unlock another ID

  **PNC will never request that a PINACLE operator have another PINACLE operator log in from the same computer during an online banking session or require another operator to log in from the same computer to reactivate/unlock an ID.**

  ▸ Experiencing problems logging in to PINACLE. Subsequently, the operator may receive a call from someone purporting to be from PNC asking for login credentials (such as a password or token passcode) or asking to have another operator log in from the same computer in order to resolve the problem

  **PNC will never ask for login credentials or request that a second user log in to resolve an issue.**

## 🛡 TAKE ACTION TO HELP PROTECT AGAINST THIS THREAT

- Verify the authenticity of the communication before opening attachments or clicking on links in any emails that are unexpected or from an unknown sender. Contact the sender at a known telephone number to confirm that the suspicious content was indeed sent to your attention.

- Use a dedicated computer with no email access and limited internet access for payment initiation or online banking access.

- Install anti-malware software.

  ▸ **PNC offers IBM® Security Trusteer Rapport® as a no-cost, optional security tool** that can help safeguard your PINACLE login credentials from phishing attempts and remove certain malware from your computer. Download and install Trusteer Rapport by visiting the link below. To learn more, please visit the PINACLE Security Center by clicking on the blue shield icon located at the upper right corner of any PINACLE page.

    **LINK:** pnc.com/en/security-privacy.html

---

▸ **If you experience any of these scenarios or if any similarly suspicious behaviors occur during a PINACLE session, your computer may be infected with malware. Please contact Treasury Management Client Care immediately at 1-800-669-1518, Option 1.**

PNC

# AVOID BEING A STATISTIC

## INCREASE THE SECURITY OF COMPUTERS AND PASSWORDS

- Use strong passwords.

- Don't recycle User IDs or passwords.

- Require password changes every 30–90 days.

- Verify that antivirus software is current and is set to update automatically.

- Install Trusteer Rapport Malware Detection Software (additional information is available in the PINACLE Security Center).

- Use dedicated computers for PINACLE access (no email and restricted website access).

## EDUCATE EMPLOYEES

- Institute cyber security and awareness training for all employees.

- Communicate new cyber trends and alerts.

- Conduct fake email campaigns to test employees' ability to recognize phishing emails.

# THE STATISTICS

**81%** of companies were targets of payments fraud in 2019.

**74%** of organizations experienced check fraud in 2019.

**75%** of companies were exposed to business email compromise (BEC) in 2019.

**37%** of organizations were subject to ACH debit fraud.

**80%** of organizations implemented education and training on the BEC threat and how to identify spear phishing attempts.

Source: 2020 AFP Payments Fraud and Control Survey — Report of Survey Results

PNC

## IMPLEMENT PAYMENTS FRAUD SOLUTIONS

The Association of Financial Professionals reported that 81% of organizations were victims of payments fraud in 2019 and adopted a stronger form of authentication or added layers of security for access to bank services.

PNC offers the following solutions:

- **Positive Pay and Payee Positive Pay**
  Matches checks presented for payment against your check issue file; those checks not matching your issue information are presented to you for a pay/return decision through PINACLE.

- **ACH Positive Pay**
  Allows you to monitor and control ACH debit activity by establishing "rules" that filter the ACH debits coming into your account(s). Using PINACLE, you review "suspect" ACH debits and determine whether to return them as "unauthorized."

- **ACH Debit Block**
  Restricts all ACH debits from posting to an account.

- **PINACLE Current Day Information Reporting**
  Provides intraday information to help you monitor activity within your accounts.

## ENHANCE INTERNAL POLICIES & PROCEDURES

- Establish formal policies and procedures for payment processing and accounts payable changes. For example:

  ‣ Require a verbal callout verification process for any vendor payment instruction change request.

  ‣ Require secondary approval (internally) for all payment requests, payment instruction changes and changes to your Accounts Payable (A/P) system.

  ‣ Use a third layer (e.g., executive approval) for high-dollar transactions.

  ‣ Segregate A/P system updates and payment initiation functions.

- Review PINACLE security features, controls and operator entitlements:

  ‣ Verify that funds movement entitlements are appropriate for each employee's job function.

  ‣ Segregate payment initiation and payment approval functions.

  ‣ Implement secondary operator approval of all entitlement changes ("2OA") for payment services.

## ADDITIONAL RESOURCES

### PNC Security & Privacy

Information and videos about current fraud trends and best practices

**LINK: pnc.com/en/security-privacy.html**

---

### PINACLE Security Center

Access to important information, updates and tips about how to keep your business safe from cyber fraud

**Click the** 🛡 **icon to log on to PINACLE**

---

### PNC Ideas, Insight & Solutions

Articles and white papers covering best practices

**LINK: pnc.com/ideas**

---

### FBI Internet Crime Complaint Center

Business and consumer fraud alerts, tools to report fraud to the FBI, frequently asked questions, tips and best practices

**LINK: www.ic3.gov
www.ftc.gov
www.staysafeonline.org**

---

### FDIC's "A Bank Customer's Guide to Cybersecurity"

What consumers can do to help protect themselves from cyber fraud

**LINK: https://www.fdic.gov/consumers/consumer/news/cnsum18/cybersecurity.html**

PNC

# CYBER SECURITY & AWARENESS
## QUICK REFERENCE GUIDE

### ☑ VERIFY AND VALIDATE

- Verify email payment or payment change requests in person or via a known phone number.
- Do not reply to an email to validate a request.
- Do not use contact information provided in an email to validate a request.
- Verify authenticity of an email before opening attachments or clicking on links.

### ⌖ PROTECT INFORMATION

- Be cautious about sharing information via social networking sites.
- Limit executive contact information on the company website.
- Do not confirm or provide personal information in response to an email or a text message.
- Do not give out personal information over the phone to unknown sources.
- Do not share executive travel/vacation schedules with unknown sources.

### DETECT BUSINESS EMAIL COMPROMISE (BEC)

- Be suspicious of any vendor change in payment instructions.
- Inspect email header and look for alterations (e.g., the use of two "Vs" to look like a "W").
- Be mindful that the "From" name in your inbox can mask a fraudulent email account.
- Be suspicious of messaging that is urgent and/or that requests secrecy.
- Be suspicious when the sender advises that they can only be reached via email.
- Be suspicious of emails requesting that payments be sent to new accounts or mailing addresses.
- Be sensitive to emotionally charged communications.
- Be suspicious of emails with generic subject lines (e.g., "Your Documents" or "Invoice").

## COMMON BEC RED FLAGS

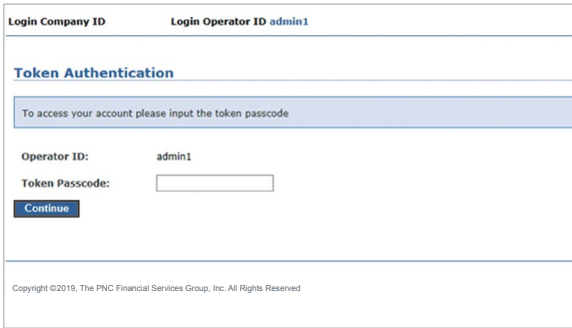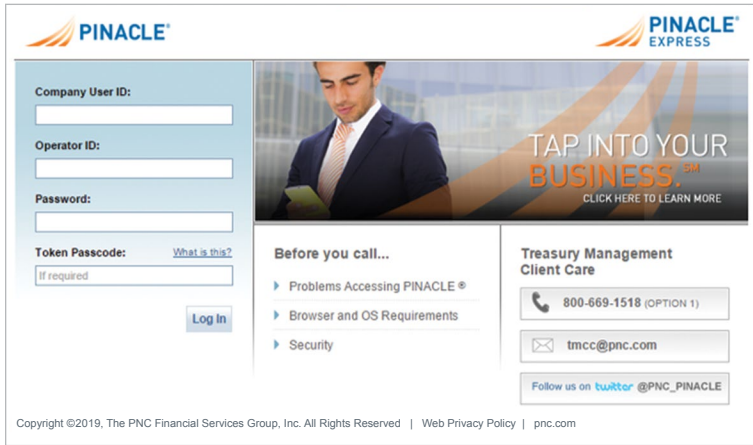| ⚠ | COMPROMISED INTERNAL EMAIL | COMPROMISED VENDOR EMAIL | FINANCIAL MALWARE | CHECK / WIRE SCAM |
|---|---|---|---|---|
| **Appears to Come From** | Company Executive | Existing Vendor | External Business Associate or Vendor | New Customer |
| **Red Flags** | • Urgent, confidential request<br>• Requestor can be reached only via email | • Requests payment using new account or payment instructions | • Email request to log into online banking using link provided in the email<br>• Online banking login:<br>  - Multiple prompts for password/token<br>  - Requires second user to log in on same computer | • Overpayment by check or card with request for refund via wire transfer |
| **Result** | • Payment sent to fraudster | • Payment sent to fraudster<br>• Vendor relationship disrupted | • Fraudster obtains login credentials and initiates payment on real bank site | • Company loss of funds reimbursed to fraudster<br>• Check or fraud payment received is invalid |

◆ PNC

# EXAMPLES

## FRAUDULENT "SPOOFED" EMAIL

| | |
|---|---|
| To | John Smith (john.smith123@gmail.com) |
| Cc: | |
| Subject: | rush payment |

**From:** John Smith mail to: john.smith@abcsteelvvorks.com
**Sent**: Wednesday, April 1, 2020 9:37 AM
**To:** Jones, Frank
**Subject:** rush payment

Frank,

Send a $77,000 payment to CompanyMMM, they are a new vendor and need to be paid immediately before they release the shipment. Wire instructions below. I am in meetings the rest of the morning, email if you have questions. Handle ASAP.

-John

Vendor: CompanyMMM
Routing Number: 555333444
Account Number: 6767671
Bank Name: Big Bank
Purpose: Shipment of goods

When you "Reply All," the email address appears differently

The "w" in the company name is spelled with two "v"s

It's an urgent request

The requestor is available only via email

## FRAUDULENT "SPOOFED" ONLINE BANKING PAGE



PINACLE®

PINACLE EXPRESS

Company User ID:

Operator ID:

Password:

Token Passcode: What is this?
If required

Log In

TAP INTO YOUR BUSINESS.℠
CLICK HERE TO LEARN MORE

Before you call...
▸ Problems Accessing PINACLE ®
▸ Browser and OS Requirements
▸ Security

Treasury Management Client Care

📞 800-669-1518 (OPTION 1)

✉ tmcc@pnc.com

Follow us on twitter @PNC_PINACLE

Copyright ©2019, The PNC Financial Services Group, Inc. All Rights Reserved  |  Web Privacy Policy  |  pnc.com

Login Company ID          Login Operator ID admin1

**Token Authentication**

To access your account please input the token passcode

Operator ID:          admin1

Token Passcode:

Continue

Copyright ©2019, The PNC Financial Services Group, Inc. All Rights Reserved

PNC

# YOUR CYBER SECURITY CONSIDERATIONS

## COMPUTER AND PASSWORDS ✓

⚠ Has your company downloaded Trusteer Rapport malware detection software that is available through PINACLE?

Does your company require regular password changes every 30 to 90 days?

Is your company's antivirus software up to date, enabled and set to auto-update?

Does your company have a dedicated computer for online banking that is not used for email or general internet browsing?

Does your company utilize any Positive Pay services?

Does your company use any other fraud surveillance tools or services?

## ENHANCED INTERNAL POLICIES & PROCEDURES

⚠ Has your executive team reinforced with your payment processing team in writing that all employees, including themselves, must strictly follow the payments processing requirements, policy and procedures?

Does your organization have formal policies and procedures in place for requesting payments and making additions/changes to your Accounts Payable (A/P) system?

Does your company require secondary approval for all payment requests?

Does your company require secondary approval for changes to payment instructions in bank and vendor payment systems?

Does your company require third-layer, executive approval for high-dollar transactions?

## VERIFY AND VALIDATE

⚠ Are email payment or vendor payment change requests confirmed by phone with the vendor using contact information on file (vs. contact information provided in the email request)?

⚠ Are payment or wire transfer requests sent via email from internal executives/managers confirmed verbally using contact information on file (vs. contact information provided in the email request)?

## INFORMATION PROTECTION

Does your company have a social media policy that employees must read and sign?

Does your company limit executive contact information on the company website?

Does your company prohibit giving out personal information, including executive travel schedules, over the phone to unknown sources?

## BUSINESS EMAIL COMPROMISE (BEC) DETECTION

Do your employees review emails for possible fraudulent payment requests, verifying headers, addresses and generic subject lines?

Are your employees cautious about email requests that are urgent and emotionally charged and when the recipient is available only via email?

## EMPLOYEE EDUCATION AND AWARENESS

Do all employees with authorization to initiate and approve payment requests receive cyber security training?

Do you provide regular alerts and updated training for employees regarding cyber trends?

PNC

## READY TO HELP

If you suspect or experience fraudulent activity, please contact PNC's Treasury Management Client Care immediately at **1-800-669-1518**, Option 1.

Or, if you would like to learn more about protecting yourself from payments fraud, contact your PNC Relationship Manager or Treasury Management Officer.