Treasury Management

# Cybersecurity Resource Guide

PNC BANK | BRILLIANTLY BORING SINCE 1865℠

# Cyberfraud Overview

## Awareness of Cyber Threats for 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 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 partner, 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 cybercriminals can obtain easily in developing such schemes. For example, large construction contracts, such as for universities or hospitals, are disclosed in public filings. Cybercriminals can access these records, register a website impersonating the legitimate contractor, and initiate communication with the university/hospital introducing a "new" accounts receivable contact and account number set up specifically for this contract. Oftentimes, the cybercriminals will wait several months before initiating contact and use open-source records to identify accounts payable personnel.

In such schemes, the cybercriminals 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. Compromised 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.

## Contents

# ⚠ 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 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 or distribution pattern for the organization 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 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.

# ⚠️ Dangerous Financial Malware Infections

Phishing emails, often with generic subject lines such as "Invoice" or "Resume," can contain dangerous 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 and Security Codes.

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

## Recognize the Warning Signs of a Malware Infection When Using PINACLE®

- A user may experience one or more of the following from a malware infection:
  - Inability to log in due to screens that delay or redirect the typical login experience.
  - Being prompted to provide their token passcode or security codes 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 codes) multiple times during the login process.**

  - Receiving instructions 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...

- **Call you or send you an email or text message asking for your PINACLE credentials or your contact information.**

- **Call you to advise you of new security procedures for your PINACLE login; we will always place this information, in advance, on the PINACLE Message Center (and you may receive a corresponding email if you subscribe to receive email alert messages).**

  **You should not respond to any communication requesting your sensitive information and should report any occurrences to TM Client Care immediately at 800-669-1518.**

## 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.

- Installing anti-malware software, which can help strengthen security measures against malicious threats, is highly recommended.
  - **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 to remove certain malware from your computer. Download and install IBM Trusteer by visiting pnc.com/en/security-privacy.html. 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.

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.**

# Recommendations and Resources

## It's Affecting Their Work

**80%**
of organizations were targets of payments fraud in 2023.[1]

**65%**
of organizations experienced check fraud in 2023.[1]

**63%**
of organizations were exposed to business email compromise (BEC) in 2023.[1]
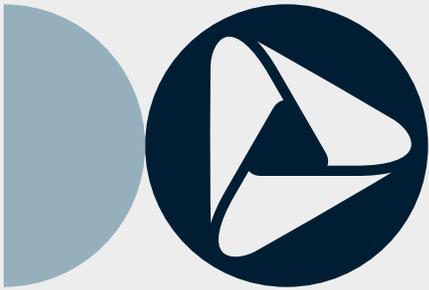
**Less than 60%** of organizations have completed the documentation that includes the creation of written policies and procedures that are required to safeguard against BEC, while **less than half (49%)** have completed testing these policies.[1]

In 2023, the FBI Internet Crime Complaint Center (IC3) received **21,489** BEC complaints with adjusted losses over **2.9 billion**.[2]

## 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 to 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 cybersecurity and awareness training for all employees, consultants and other third-party administrators.
- Communicate new cyber trends and alerts.
- Conduct fake email campaigns to test users' ability to recognize phishing emails.

## Implement Fraud Solutions

Our product and solution professionals can work with you to understand your company's needs and recommend specific services and optional service features to help your company enhance its fraud prevention posture. **Below are just some of the services that we offer:**

**PNC Verification Services**
A service that can help you confirm critical information regarding the identity and bank account of your intended payees prior to facilitating a payment; helps to reduce fraud losses brought about by imposter fraud scams and administrative costs incurred with returned items.

**Check Positive Pay**
A service that matches checks presented for payment against your company's check issue file; "exceptions" are presented to you for a pay/return decision through PINACLE, PNC's top-rated corporate online and mobile banking platform. PNC's Positive Pay service includes teller line coverage and payee verification.

**ACH Positive Pay**
A service that 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 can review "suspect" ACH debits and determine whether to return them as "unauthorized."

**ACH Debit Block**
A service that restricts any ACH debit transactions from posting to an account.

**PINACLE Current Day Information Reporting**
A service that provides intraday information to help you monitor activity within your accounts.

**PINACLE Event Notifications**
A service that allows you to subscribe to receive notifications about key activities within PINACLE that can be delivered to the PINACLE Message Center, or directly to you via email or text message.

**Commercial Card Payments**
An electronic payment option that reduces fraud exposure by allowing you to set spending controls while leveraging transaction monitoring against spending habits that will trigger a fraud alert for suspect transactions.

**Invoice Manager Pro**
A service that can help you avoid processing unauthorized invoices. PNC can capture your invoices, monitor for duplicates, and compare your invoices to your vendors and purchase orders to ensure the invoices you pay are legitimate.

**Check Print Outsourcing**
A service that aims to provide check printing in a secure environment using check stock with multiple security features. Check information is automatically integrated into PNC's Check Positive Pay service.

**Customized Accounts Receivable Reporting and UPIC
(Universal Payment Identification Code)**
PNC offers multiple virtual account solutions that allow you to receive electronic payments to your bank account without having to reveal your bank account number.

**IBM Security Trusteer Rapport\***
A software application that provides an additional layer of security designed to help protect your login credentials, including your PINACLE Company ID, Operator ID and password.

**\***By clicking "Download," you will be directed to a third-party website hosted by Trusteer, a third party that is not affiliated with PNC Bank. While this software is a valuable addition to your fraud prevention strategy, PNC Bank will not be responsible for the content or effectiveness of the services associated with Trusteer's software.

## Enhance Internal Policies and Procedures

**Establish formal policies and procedures for payment processing and investment changes. For example:**

• Require I-Hub usage or have a verbal callout verification process for any payment or distribution instruction change request.

• Require secondary approval (internally) for all withdrawals, transfers and other significant changes.

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

**Review I-Hub security features, controls and operator entitlements:**

• Confirm that funds movement entitlements are appropriate for each employee's job function or role.

• Review notification settings to ensure that withdrawals exceeding certain thresholds generate emails to all authorized users.

• Segregate payment initiation and payment approval functions.

## Additional Resources

**PNC Security & Privacy**
Information and videos about current fraud trends and protocols

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

**PINACLE Security Center**
Access to important information, updates and tips to improve your fraud mitigation strategy

**Click the**  **icon at the top right of any PINACLE page**

**PNC Ideas, Insights & Solutions**
Articles, white papers and insights

**pnc.com/insights/cib**

**FBI Internet Crime Complaint Center**
Business and consumer fraud alerts, tools to report fraud to the FBI, frequently asked questions, tips and considerations

**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 cyberfraud

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

# Cybersecurity and Awareness
## Quick Reference Guide

⚠️ **Common Business Email Compromise Red Flags**

| | Compromised Internal Email | Compromised Vendor Email | Financial Malware |
|---|---|---|---|
| **Appears to Come From** | Organization Executive | Existing Vendor | External Business Partner or Vendor |
| **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 in to 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 |
| **Result** | Payment sent to fraudster | • Payment sent to fraudster<br>• Vendor relationship disrupted | Fraudster obtains login credentials and initiates payment on real bank site |

## Verify and Validate

- Verify email payment/distribution or payment/distribution 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 your organization's 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 change in a vendor's payment instructions.

- Inspect email header and look for alterations (e.g., the use of two "V's" 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 be reached only via email.

- Be suspicious of emails requesting that payments or transfers 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").

## Fraudulent "Spoofed" Email | Example

| To | John Smith (john.smith123@gmail.com) |
|---|---|
| Cc: | |
| Subject: | rush payment |
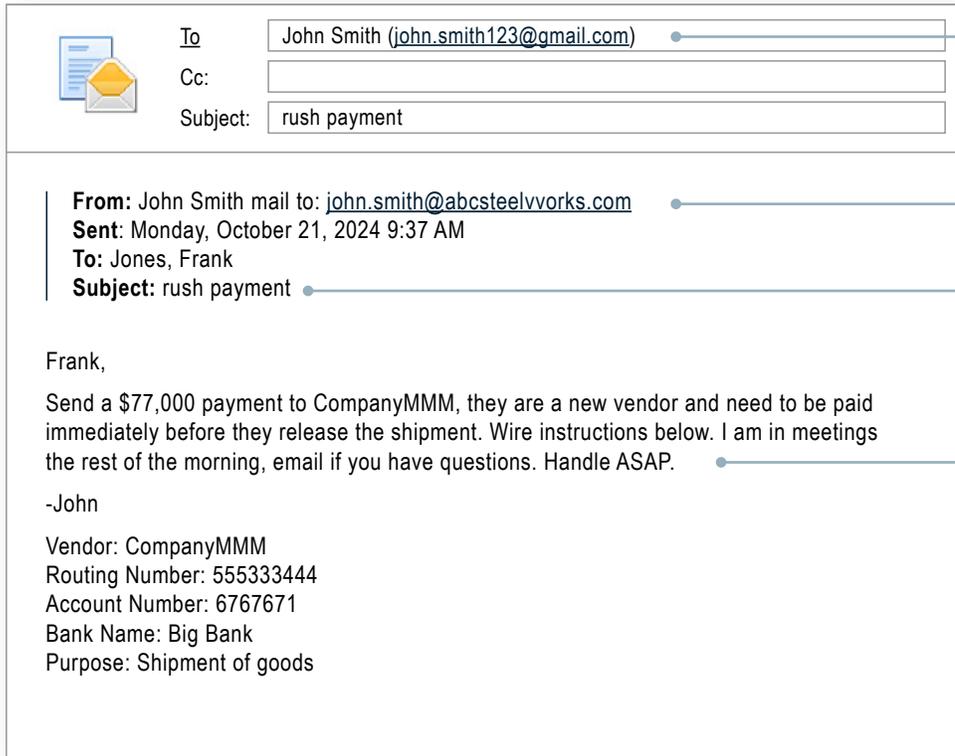
**When you "Reply All," the email address appears differently**

**From:** John Smith mail to: john.smith@abcsteelvvorks.com
**Sent**: Monday, October 21, 2024 9:37 AM
**To:** Jones, Frank
**Subject:** rush payment

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

**It's an urgent request**

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

**New wire instructions not currently on file**

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

## Webpage Spoofing

Whether through malware infection or domain spoofing, the cybercriminals' ultimate goal is to redirect web traffic away from a legitimate website to a spoofed version of that site. Once on the spoofed site — believing it to be the legitimate site — the target enters their credentials and other sensitive information, attempting to log in to the site. In turn, the cybercriminals use information entered by the target on the spoofed site to log in to the legitimate site, upon which they can gain access to whatever information or tools the target may have.
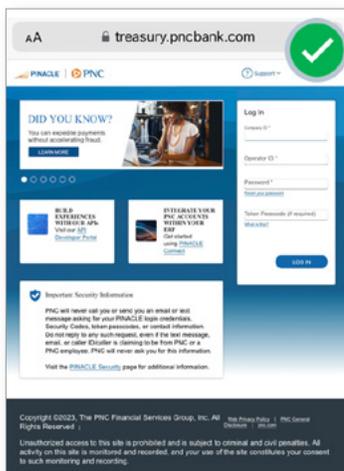
**Actual PINACLE login page**

We recommend accessing online banking sites like PINACLE with bookmarks or shortcuts as opposed to using a search engine to navigate to those pages.
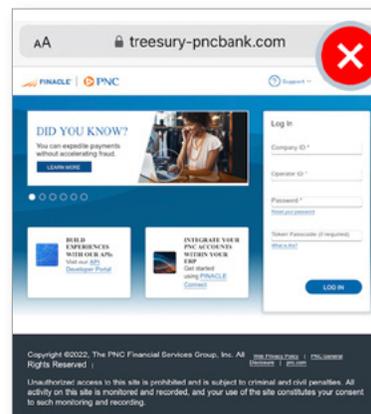
**Spoofed PINACLE login page**

- Unrecognized URL
- Omission of the "Important Security Information" box

## Phishing

Using email, cybercriminals will send messages containing a link to a malicious website or a malware-infected document attachment to their target. Upon the target's receiving the email and clicking on the link or opening the attachment, unbeknownst to them, the malware will automatically install on their device. In many cases, the malware is designed to redirect web traffic away from a legitimate website to a spoofed version of that site used to harvest login credentials or other sensitive information entered on the site by the cybercriminals' target.

**Message is designed to elicit an emotional response**

**Vague sender name**

**Improper or incomplete branding**

**Inclusion of a web link or document attachment**

**Grammatical and punctuation errors**

**Formatting or layout anomalies**
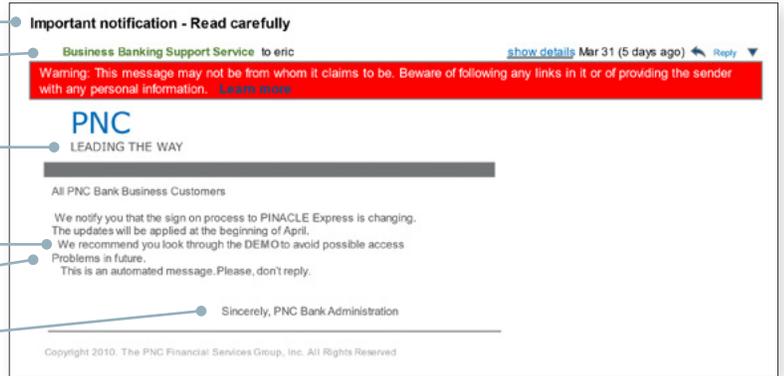


## Domain Spoofing

In addition to attempting to install malware to their targets' devices through phishing and smishing scams, cybercriminals may plant spoofed web links on the open web by purchasing advertisements appearing in search engine results page.

**Unrecognized URL**

**Improper branding (e.g., "P.N.C" vs. "PNC")**

**Grammatical and/or punctuation errors**

**Confusing, illogical and/or nonsensical site description**
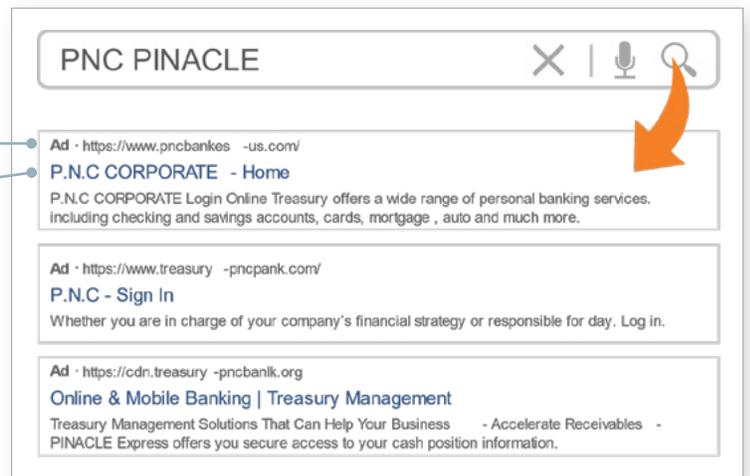
## Smishing

Similar to phishing, with smishing, cybercriminals will send text messages containing a link to a malicious website or a malware-infected document attachment to their target.

**Unrecognized SMS short code (i.e., sender's phone number)**

**Improper branding (e.g., "Pinacle" vs. "PINACLE")**

**Inclusion of a web link or document attachment**

**Directing to a generic/odd contact for service**

> <#>PNC Pinacle Alert: ABC Corp. Did you just attempt $17,550.00 via ACH to Coinbase.com for bitcoin crypto currency? Reply 1 for yes or reply 2 for no. Any questions call us at the number on the back of your card. Reply STOP to opt out of fraud alerts. Data rates may apply.

### Add PINACLE's short codes to your contacts to help identify and avoid engaging with smishing attempts:

**PINACLE Security - 76200**
You will receive Security Codes from this short code when logging in to PINACLE or updating your PINACLE user profile information.

**PINACLE Event Notifications - 762242**
You will receive Event Notifications from this short code if you subscribe to SMS delivery. Notifications may include authentication-related actions, balance and transaction details, payment approvals, payment status changes, and positive pay exceptions.

**Commercial Card - 762411**
You will receive messages from this short code for Commercial Card information. Messages may include next payment due, payment made, declined transactions and daily balance activity as well as fraud alerts asking for confirmation regarding a specific card transaction.

**ePayments - 26489**
Your Payees will receive notifications and reminders to facilitate payment selection based on your payment instructions.

# Cybersecurity Checklist
## Your Cybersecurity 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 and Procedures

| | |
|---|---|
| Has your executive team reinforced with your payment processing team in writing that all employees, including themselves, must strictly follow the payment 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 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/Third-Party Education and Awareness

| | |
|---|---|
| Do all employees with authorization to initiate and approve payment requests receive cybersecurity training? | |
| Do you provide regular alerts and updated training for employees regarding cyber trends? | |

# Additional Recommendations

- Create and manage rules and alerts in PINACLE to monitor and manage time-sensitive activity.

- Regularly review user limits and permissions within PINACLE.

- Monitor your account for unexpected micro deposits and/or small dollar payments.

- Subscribe to Positive Pay service.

**Once subscribed to Positive Pay:**

- Submit complete, accurate and timely check issue information to the bank for processing.

- Log in to PINACLE each business day to review and decision positive pay exceptions.

- Reduce your risk of financial loss by setting the positive pay exceptions default decision to "Return."

## Brilliant begins here

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.

**pnc.com/treasury**

PNC BANK | BRILLIANTLY BORING SINCE 1865 ℠