Cyber and electronic payments fraud.

KeyBank

Schemes and Red Flags

Scheme	What Happens	Red Flags to Watch For
Business Email Compromise (BEC)	Fraudsters spoof and/or compromise known business email accounts, impersonating executives, company personnel, or known vendors to request fund transfers to fraudulent accounts.	• Payment requests to new accounts • Unusual, often urgent, instructions • Unusual vendor invoices • Out-of-character vendor behavior • Typos in email
Phishing Scams	Fraudsters use emails, mail, phone calls, QR codes, text messages and more to trick employees into sharing sensitive information, such as login credentials or financial data.	• Requests for login credentials or bank account information • Suspicious email details, information, links, QR codes, or attachments **KeyBank will NEVER ask clients for their login credentials.*
AI Deepfake Fraud	AI-generated (artificial intelligence) audio or video mimicking executives, company personnel, or vendors who authorize fraudulent transactions or share sensitive information.	• Unusual executive or business partner requests • Unwillingness with authentication practices • Inconsistencies in audio or video • Deviations from normal behavior
Account Takeover and Double-Sided Spoofing	Fraudsters impersonate trusted entities and/or steal login credentials to access your company bank account or data, including financial systems and/or company emails.	• Unauthorized transactions appear in the bank account • Increased security alert notification • Manipulative tactics, also known as social engineering, to gain access to sensitive information
Insider Fraud	Employees or contractors misuse access to company systems for fraudulent activity.	• Employee behavioral changes (i.e., unusual working hours, defensive behavior) • Unusual data access patterns • Irregular account transaction activity
SIM Swapping	Fraudster takes control of a victim's phone number by transferring it to a new SIM card, allowing the interception of calls and messages.	• Sudden unexpected loss of cell service • Unexpected calls or texts • Calls and/or texts not coming through • Applications do not recognize your device
Ransomware	Fraudsters use malware to encrypt a company's data or overwhelm a company's servers with traffic and demand a ransom to stop the attack.	• Suspicious emails and communication • Unusual security system alerts (slowness, firewall changes, pop-up warnings, etc.) • Suspicious network activity (traffic, data transfers, etc.)

How can you protect yourself?

KeyBank

Educate Employees Inform employees about schemes and how to identify them. Regular employee training is recommended.	**Suspicious? Don't Reply** Never reply directly to suspicious emails. (Fraudulent emails will be different by a character.) Instead, reach out to a known contact using known contact information and do not use contact information provided in any suspicious emails.	**Authenticate** With the rise of AI-generated scams, take the extra minute to properly authenticate the person and the validity of the request.
Stay Vigilant Be suspicious of red flags such as negative reactions to probing questions, frustration or hesitancy to comply with authentication, and typos in requests (names, email domains, etc.).	**Safeguard Information** Never share user credentials (i.e. usernames, passwords, etc.). Use enhanced methods of login credentials. Update passwords on consistent basis. Never post payment instructions publicly.	**Validate Payment Instructions** Verify any new or changed payment instructions or invoices with a known contact before making payments. Call known number, not number on invoice.
Multi-Layer Approval and Authentication Implement multi-layer payment approval process (initiator and approver) and recommend your business partners/vendors use multi-factor authentication before processing requests.	**Confirm Payment Receipt** Immediately after a payment is made, contact the known vendor/payee to confirm receipt of the payment.	**Monitor and Escalate** Review your account activity daily for unusual behavior, and if a scam is suspected, escalate the situation immediately, both internally and to your KeyBank relationship team.
Utilize Products and Tools Review the suite of fraud solutions with your relationship team and help ensure you have products that protect your account activity.	**Set Up/Review Online Alerts** Set up appropriate account alerts on your KeyBank online banking profile to get notified of any abnormal account behavior. Take this action for all user account profiles.	**Set Limits** Set financial transaction limits based on your business needs and requirements.

If you believe you are a victim of fraud, please take the following steps:

- Contact the Key Fraud Client Service Center at 800-433-0124. Dial 711 for TTY/TRS.
- Contact law enforcement.
- Contact your Relationship Manager or Payments Advisor.