Arming Against Cyber Threats:

Essential Tools & Strategies

June 2026

Todd Dahmann, Vice President
Cybersecurity & Technology Controls, Exercises & External Engagements

JPMorganChase

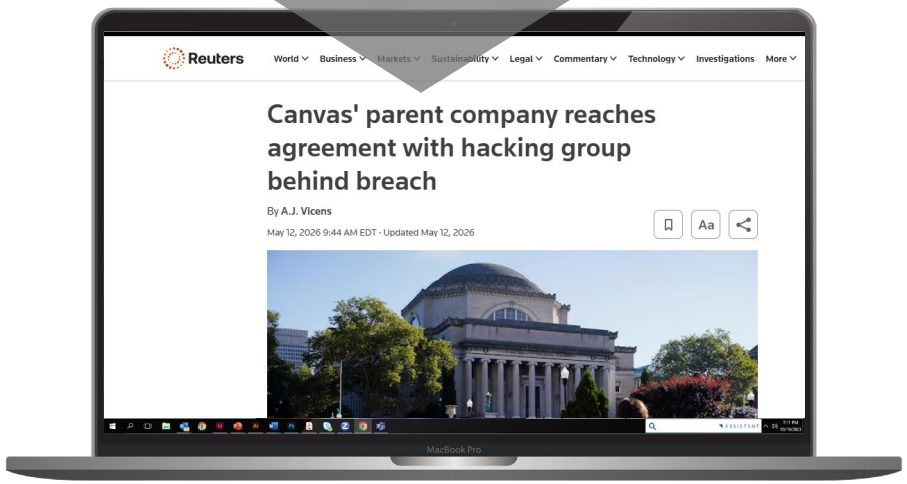
DISCLAIMER

This information is provided for discussion 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 is 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. JPMorgan Chase assumes no responsibility or liability whatsoever to any person in respect of such matters. Further, the content may not be copied, published, disclosed or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan Chase.

Bad actors continuously seek to leverage emerging technology and vulnerabilities to carry out malicious activity…

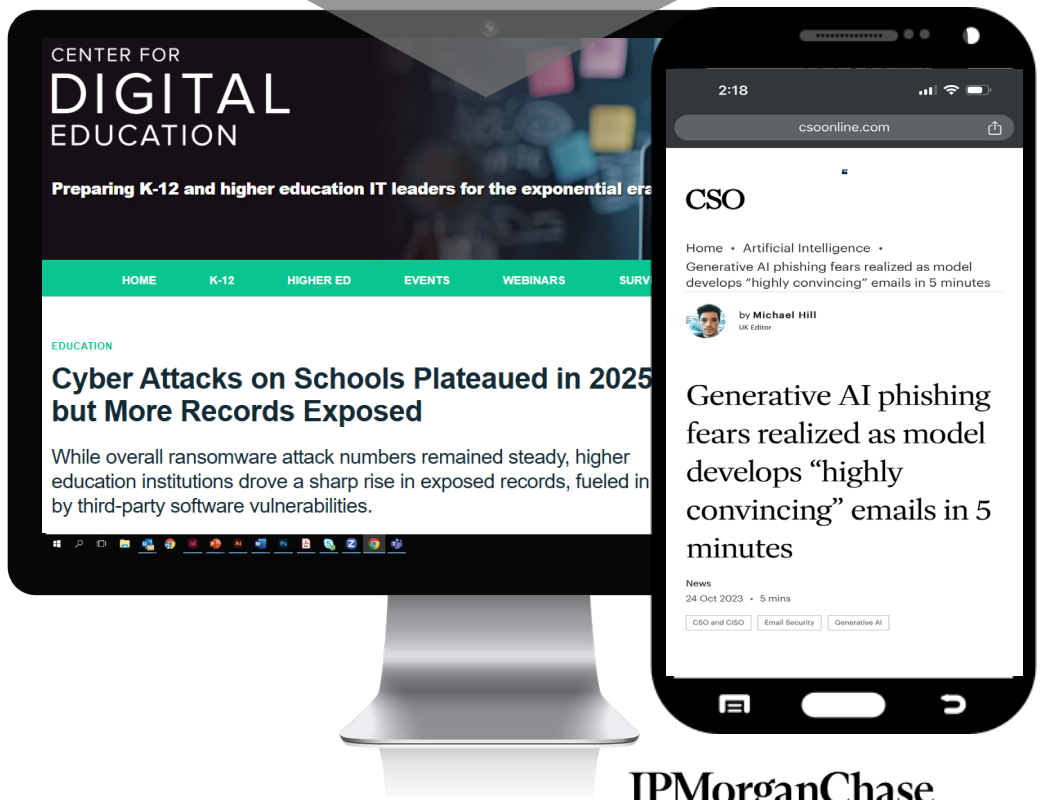
… an estimated 9,000 institutions in the US, Canada, Australia and the UK, with exams disrupted…

Shiny Hunters threatened to publish 3.5 terabytes of data they had stolen in the breach.



While overall ransomware attack numbers remained steady, higher education institutions drove a sharp rise in exposed records, fueled in part by third-party software vulnerabilities.

February 13, 2026 • Abby Sourwine

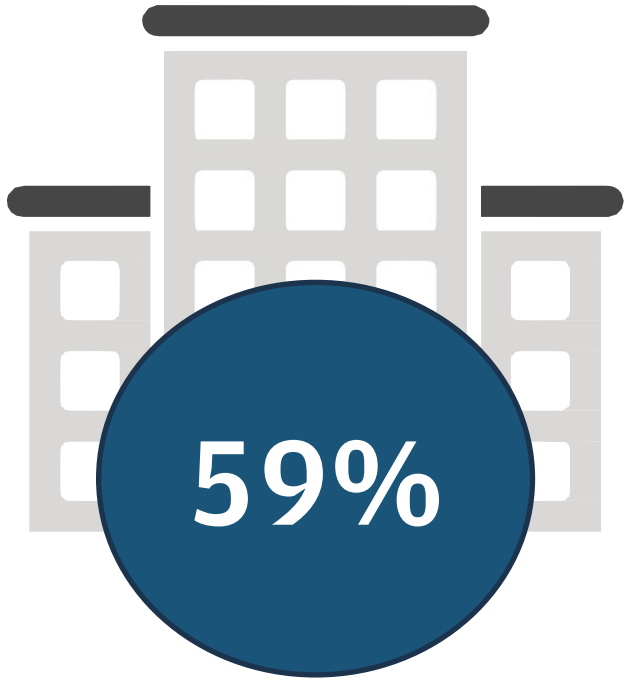


JPMorganChase

This activity adds to an already-growing threat landscape that has seen increased attacks...

703%

Increase in credential phishing attacks in H2 2024[1]



Companies that have completed an enterprise-wide fraud risk assessment in the last 12 months[4]

98%

Organizations are affiliated with a 3rd party that has had a data breach[2]

70%

Percentage of organizations that distrust their current internal controls to prevent payment fraud[3]

42%

Global organizations do not have a 3rd party risk management program[4]

1. Security Staff. (2024, December). Credential phishing attacks rose by 703% in H2 of 2024. Security Magazine. https://www.securitymagazine.com/articles/101261-credential-phishing-attacks-rose-by-703-in-h2-of-2024
2. Security Staff. (2024, December). Third-party attack vectors are responsible for 29% of breaches. Security Magazine. https://www.securitymagazine.com/articles/100447-third-party-attack-vectors-are-responsible-for-29-of-breaches
3. Ponemon Institute 2023 Report
4. PWC. (2024). Global Economic Crime Survey 2024 . Global Economic Crime Survey. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

JPMorganChase

Threat Landscape: Addressing Today's Top Cyber Trends

Cyber Threats Are Constantly Evolving

Supply Chain Compromise

Threat actors compromising an organization by targeting less secure partners of its supply chain. Rampant increase in Year over Year supply chain attacks.

Managing the Risk: Supplier Threat Intelligence, Third-Party Oversight, Asset Management, Vulnerability Management, Business Continuity Panning and identification of resilient alternatives (e.g., in house service)

Malware and Ransomware

Ransomware as a Service model enables cyber criminals to encrypt systems with ransomware and extort victims.

Managing the risk: Antimalware, Data Backup and Recovery, Email and Web Content Filtering, Access Controls, Cyber Threat Intelligence, Security Monitoring, Digital Forensics

Social Engineering

Sophisticated Phishing, Smishing and Vishing campaigns are increasing with the use of AI. Vast majority of incidents start with social engineering.

Managing the risk: Security Awareness training, Email and web content filtering, Access Controls, Antimalware, Security Monitoring, Brand management services to prevent spoofing

Distributed Denial of Service (DDoS) & Internet Of Things (IOT) Attacks

DDoS attacks disrupt availability of services with flood of malicious Internet traffic. Compromise and abuse of insecure IOT devices to conduct DDoS attacks or gain access to networks.

Managing the risk: Inline DDoS protection, Cyber Threat Intelligence to monitor campaigns and targeting, Asset & Inventory Management, Network Access Controls

Disinformation and Artificial Intelligence (AI) Abuse

Improper use of AI and synthetic media to deceive end users and perpetrate fraud. Increasing financial losses across payments and treasury departments.

Managing the risk: Awareness and fraud prevention training, collaboration with government and law enforcement, enhanced payment verification controls, investment in AI/emerging tech

Data Loss and Breaches

Loss of confidential information as a result of internal (e.g., human error or malicious insider) and external threats

Managing the Risk: Data Loss Prevention, Blocking removable media, Information Classification and Handingling, Access Controls, and Data protections (e.g., encryption)

The Power of Artificial Intelligence

AI can empower business to drive growth in an increasingly competitive business landscape

Automated Processes

Data-Driven Insights

Personalization

$4.4T

Major Financial Impact

Added to the global economy annually[1]

OPPORTUNITIES

- Automation and Efficiency
- Data Analysis
- Customization
- Enhanced Security
- Analytics and Forecasting
- Innovation
- Process Optimization

CHALLENGES

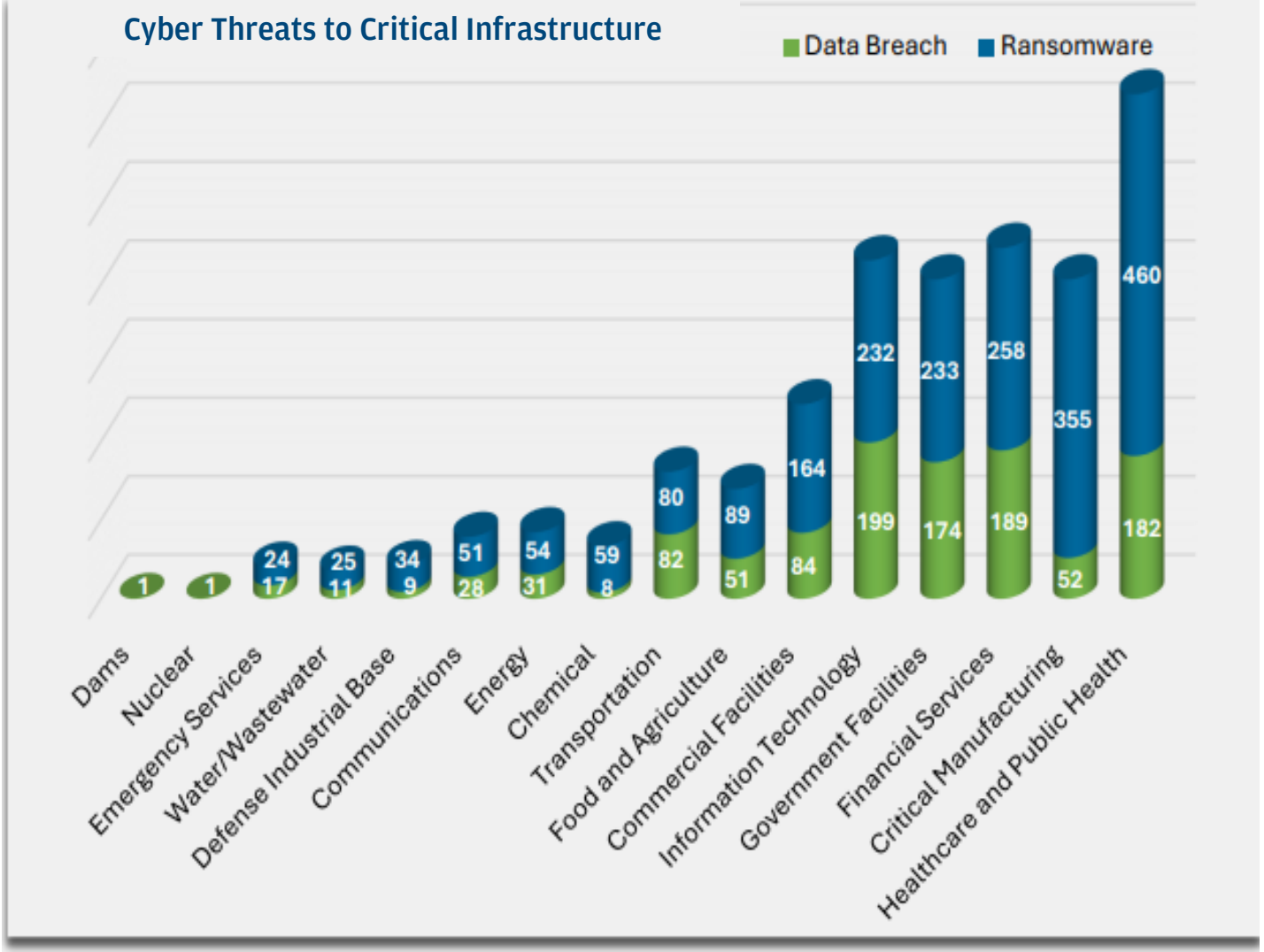
- Data Quality
- Talent Gap
- Ethical Considerations
- Integrating Systems
- Trust
- Cybersecurity
- Cost and ROI

CYBER & FRAUD THREATS

- Data Breaches
- Model Poisoning
- Bias and Discrimination
- Account Takeovers
- Synthetic Identity Fraud
- Insider Threats
- Deepfake Threats

[1] McKinsey & Company, *The economic potential of generative AI*, June 2023

Some are targeted more than others…



Cyber Threats

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.

Cyber threats include ransomware, viruses and malware, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the U.S., their incapacitation or destruction would have a debilitating effect on national security, economic security, or public health and safety.

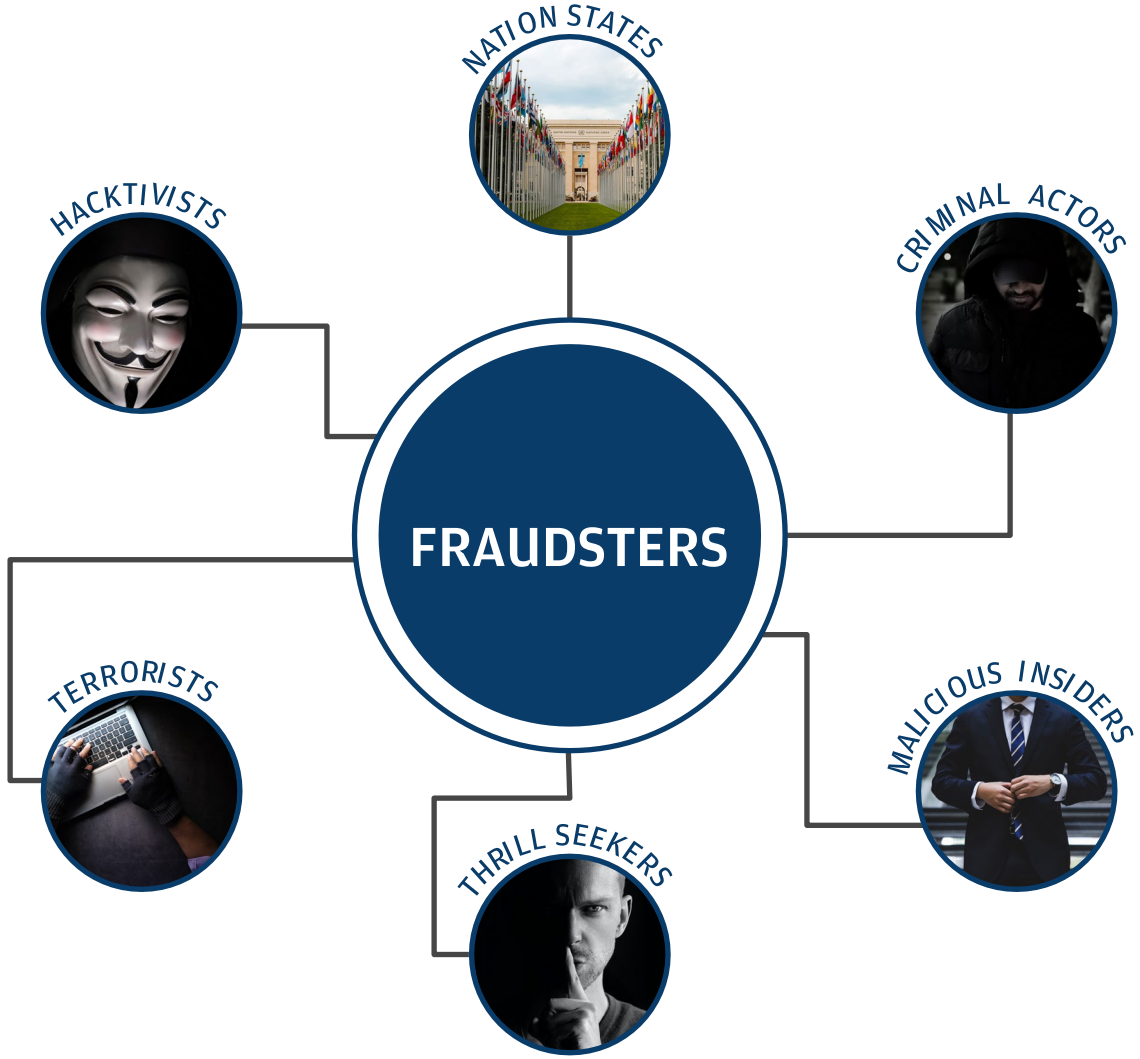
Read More – https://www.cisa.gov/topics/critical-infrastructure-security-andresilience/critical-infrastructure-sectors

Non-Critical Sector Ransomware Reporting		
IC3 received more than 1,400 ransomware complaints from businesses and organizations not related to a critical sector. Below are the most reported industries for these complaints.		
		Example
18%	Legal services	law firms, estate planning
17%	Contracting services	electricians, general contractors
10%	Engineering, architectural services	engineering firms, land surveying
7%	Consulting services	project management, marketing services
5%	Non-critical manufacturing	furniture, building materials

FBI 2025 IC3 Report - https://www.ic3.gov/AnnualReport/Reports/

Who Commits Fraud?

- Not all fraudsters are the same. Some are criminals or part of criminal organizations that are motivated by money and self-interest
- Some fraudsters are motivated by revenge and a desire to get back for perceived sights
- Other fraud actors are part of nation-states or terrorist groups that conduct attacks to enrich their home country or to harm the victim country
- Other actors may be motivated by the thrill of conducting illegal activity or by seeing what they can get away with



Top 10 Internet Crimes of 2025

US Loss by Complaint

Crime Type	Loss
Investment	$8,648,617,756
BEC	$3,046,598,558
Tech/Customer Support	$2,134,675,818
Personal Data Breach	$1,314,923,988
Confidence/Romance	$785,436,888
Government Impersonation	$672,009,052
Other	$405,624,084
Non-Payment/Non-Delivery	$364,855,818
Data Breach	$264,223,271
Employment	$199,889,841

Florida Loss by Complaint

Crime Type	Loss
Investment	$678,631,427
Tech Support	$179,266,125
BEC	$187,280,919
Personal Data Breach	$122,522,988
Confidence/Romance	$75,466,953
Data Breach	$48,052,463
Other	$46,553,963
Non-payment/Non-Delivery	$39,688,154
Real Estate	$30,863,761
Identity Theft	$30,151,099

FBI 2025 IC3 Report - https://www.ic3.gov/AnnualReport/Reports/

Common Payment Fraud Scenarios

Vendor & Executive Impersonation

Impersonation tactics used to deceive organizations into fraudulent payments. Business Email Compromise is a common tactic

Third-Party Compromise

Occurs when an organization's vendor or supplier is hacked leading to the manipulation of billing details or bank accounts, resulting in fraudulent transactions

Account Takeover

When an attacker gains unauthorized access to a corporate bank account, often using stolen or compromised credentials to make unauthorized transactions

Malicious Insider/User Entitlement Fraud

Intentional actions by current or former employees or contractors, where they gain access to accounts to manipulate payments

Systems and Human Error

Although not fraud, these unintentional errors can cause financial losses. This includes instances where someone inputs incorrect payment information

Sanctioned Entities

Payments made to sanctioned entities, resulting in potential legal repercussions, financial losses, and reputational damage

AI is being leveraged by threat actors to aid their social engineering capabilities…

Sophistication

- More convincing and formal wording
- No more language barrier
- Undermines historical indications of phishing/scams (misspelled words, poor grammar, etc.)
- Greater accessibility and a lower barrier of entry

Best practice

- Increase scrutiny around potential phishing emails and messages from other channels
- Continuously train and test employees
- Use multifactor authentication to prevent attackers from getting in using legitimate credentials

Deepfake

- Video, audio, and image deepfake technologies are improving rapidly
- Real-time capabilities for impersonation
- Bypassing remote identity verification systems such as facial recognition or voice authentication

Best practice

- Limit audio and video exposure on publicly accessible platforms – even small snippets can be used to create a deepfake
- Do not rely solely on voice or video authentication
- Follow established procedures around payments and account changes

Automation

- Can be used for phishing, misinformation, & social media campaigns
- Increases efficiency for attackers and allows for higher volume attacks
- Intelligence gathering using data mining across different platforms (social media, public records, etc.)

Best practice

- Use and verify trusted sources for information and news
- Update privacy settings on social media and other publicly visible accounts; use a VPN
- Limit the amount of personal content posted to social media

AI is being leveraged by threat actors to enhance their efforts…

Increased efficiency, automation, and a lower barrier of entry allow for unprecedented capabilities

Social engineering

AI bolsters attackers' social engineering capabilities, undermining conventional ways of identifying these attacks

- Automation for phishing, misinformation, & social media campaigns
- Improved grammar (no more language barrier), more convincing wording, increased sophistication, easier spoofing
- Deepfake capabilities for voice and/or video

Malware development & Malicious AI

Attackers can exploit existing AI programs or use malicious AI tools to aid in the development and dissemination of malware

- Automated distribution of malware
- Vulnerability scanning on target systems
- Malware & polymorphic malware generation
- WormGPT, SpamGPT & FraudGPT

Attacks against AI/ML systems

Threat actors continue to develop ways to thwart AI systems through a range of adversarial techniques:

Poisoning attacks

Target training data or data labels, handicapping the model during or after deployment

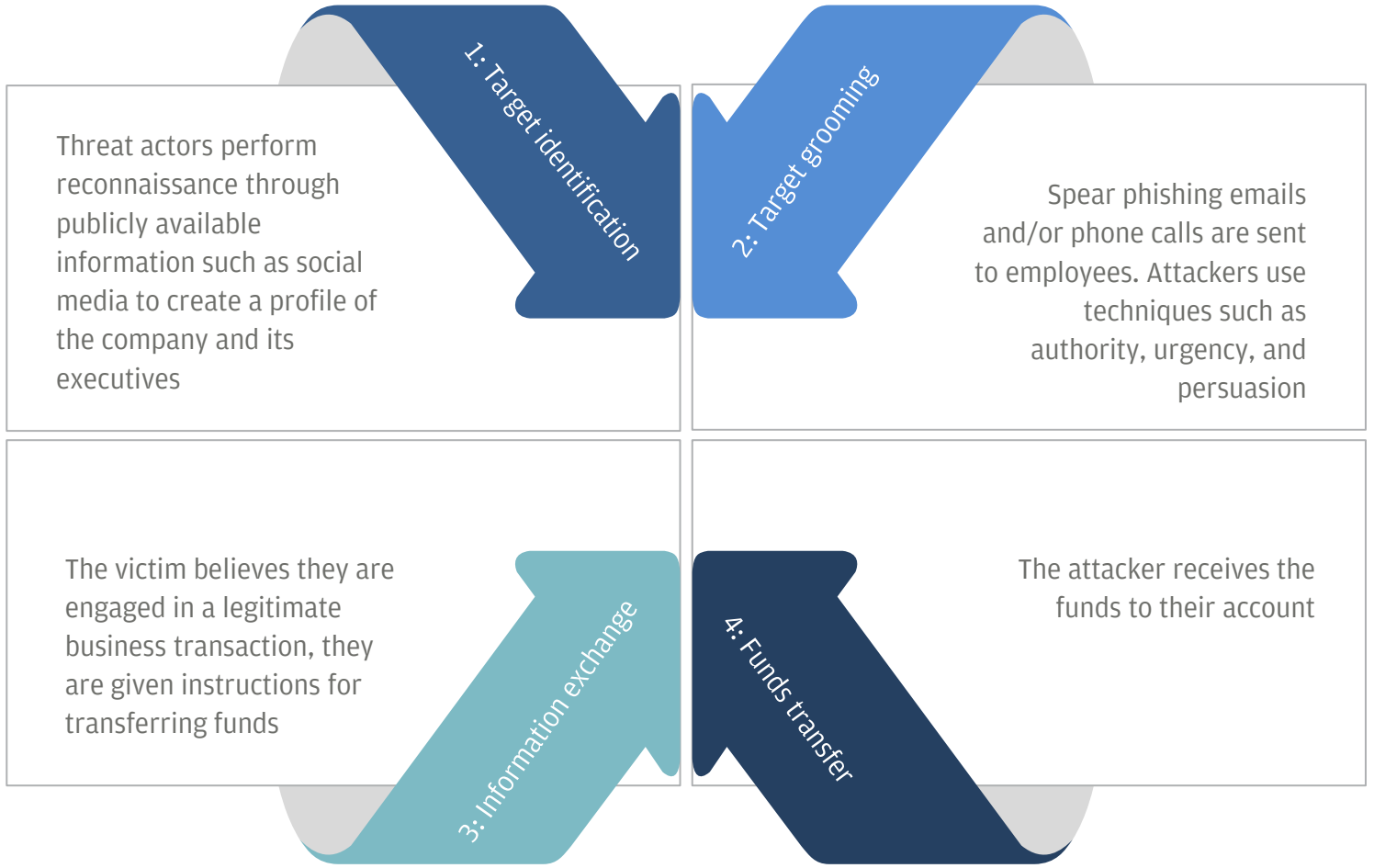
Evasion attacks

Manipulate data during deployment to avoid detection by previous training classifiers (often used in intrusion and malware scenarios)

Model extraction attacks

Probe the target model to reconstruct it or steal the training data

BEC Timeline & Top Targets



Executives

Publicly accessible information likely available via social media and company websites; high authority level within company structure

Finance/Treasury

Knowledge on banking and payment details; ability to execute funds transfers

HR

Access to employee records/information

New Employees

Less familiar with company relationships; less experienced with company protocols

Identifying Business Email Compromise (BEC) and Phishing

Examples

Email Spoofing / Masking: A spoofed or masked email contains a forged email header that hides the true origination of a message

- *Fraudsters trick employees of victim companies into divulging company sensitive information and/or initiating payments based on fraudulent instructions*

Client Email Compromise: Fraudsters compromise an employee's email account at a victim company; often referred to as account takeover or hacking

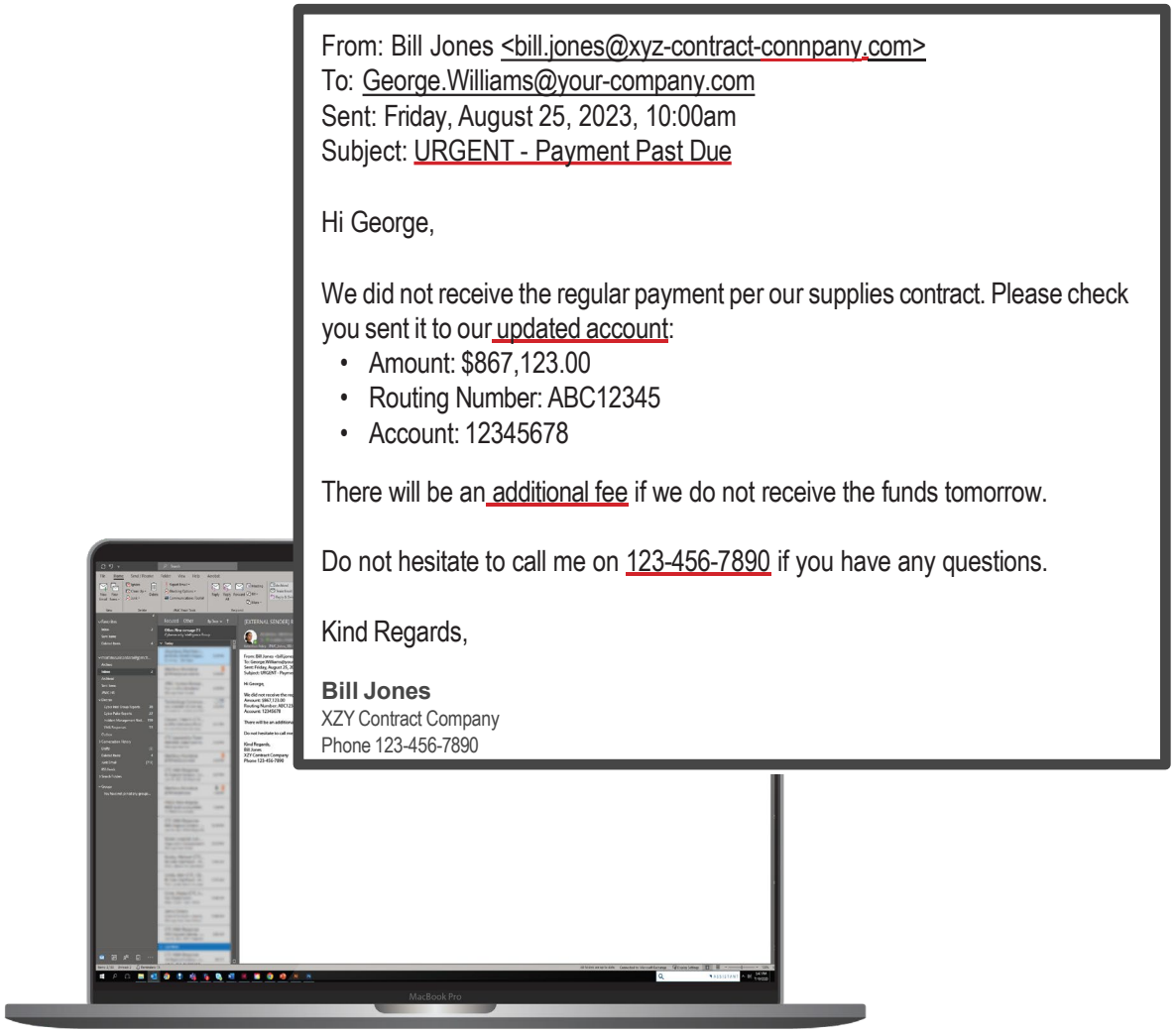
- *Fraudsters exploit email or network access to mimic a client's communication style and deceive a business into making fraudulent payments*

Vendor Email Compromise / Supply Chain: Fraudsters impersonate a company's vendor rather than a company's employee

- *Similar to a Client Email Compromise, a vendor's clients receive requests with updated accounts; the client then send funds to what they believe to be a valid account from their trusted vendor*

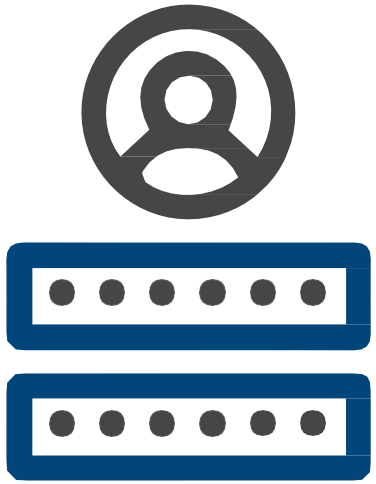
Lookalike Domain: Fraudsters purchase/register a domain closely resembling the legitimate company's, then setup a related email account to target the victim company

- *Victim companies' employees often do not notice the difference between their legitimate corporate domain and the lookalike which is visually very similar*



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
- Make sure **multiple users do not log in from the same computer** to initiate or release payments
- Use approved templates/verified bank lines and **restrict use of free form payments**

Verification

- Make sure **money is not moved based solely on an email or telephone instruction(s),** even from trusted vendors
- Try to **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**
- Use **multi-factor authentication (MFA)** wherever possible

Reconciliation

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

Detection

- Be sure to **Identify** irregularities (e.g., first time beneficiaries, cross-border payments)
- Always **verify** payment **values**, **volume** and **velocity**
- Establish criteria to **validate** or release payments
- Continually **Track and trace** payments to detect modification

JPMorganChase

Resiliency is paramount in the face of today's evolving threats…

"Everybody has a plan until they get punched in the mouth"

Awareness of the Threat Landscape	Taking a proactive approach to identifying threats and assigning the appropriate risk and priority levels Understanding the tactics, techniques and procedures employed by adversaries to defend against them effectively
Implementing new Technologies	Investing in new technologies such as post-quantum cryptography, AI/ML, next-generation firewalls, and more, to vouchsafe organizational security into the future
Employee Training and Education	Fostering and promoting a culture of reporting and awareness; training and testing regularly
Incident Response	Clearly defining roles, responsibilities, and procedures to ensure timely response and recovery while minimizing incident impact and maintaining operational capabilities
Collaboration with Industry Partners	Sharing intelligence and collaborating on solutions for mutual benefit and preparedness across the industry
Continuous Assessment and Improvement	Stress testing security controls and response plans on a regular basis to match the dynamic threat landscape

QUESTIONS?

WHITEPAPERS & WEBINAR REPLAYS:
jpmorgan.com/commercial-banking/insights/cybersecurity

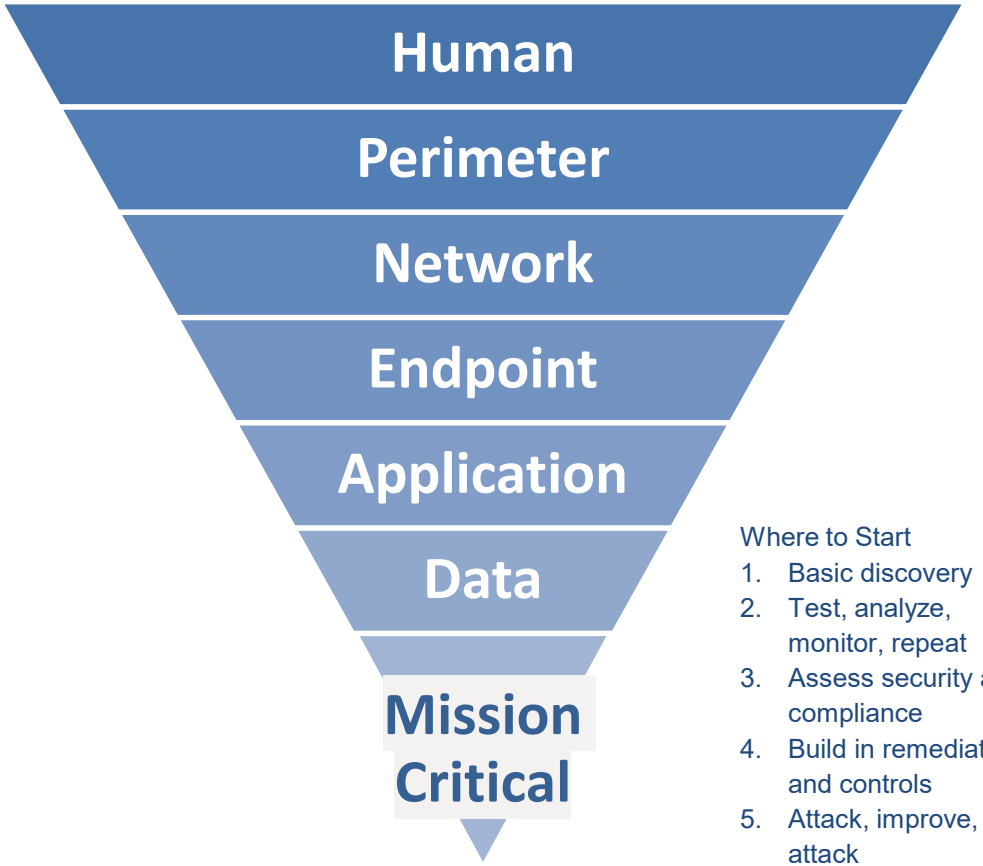
Appendix

Additional Resources:

www.IC3.gov - FBI Internet Crime Complaint Center – See “resources”
www.CISA.gov - Critical Infrastructure Security & Resilience – See “Resources & Tools” –
Also, See https://www.cisa.gov/cyber-guidance-small-businesses

Defense in Depth

Companies should build and leverage technology to detect fraudulent activity and attacks across high and low value asset types.



Where to Start

1. Basic discovery
2. Test, analyze, monitor, repeat
3. Assess security and compliance
4. Build in remediation and controls
5. Attack, improve, attack

Layer 7 (Human):
Phishing tests, social engineering training, access management controls

Layer 6 (Perimeter):
Physical security, industry intelligence, malware, endpoint security & brand protection

Layer 5 (Network):
Unauthorized access, zero trust, API configuration

Layer 4 (Endpoint):
Protect network and additional unauthorized access

Layer 3 (Application):
Protect applications, Software Development Life Cycle (SDLC) and internal app security

Layer 2 (Data):
Security controls, in transit and at rest

Layer 1 (Mission Critical):
The organizations most critical data

Insights: Best Practices to Protect Your Firm

Independent Assessment

Engage an experienced Firm that understands the technical risks, complexities of enterprise architecture for a technical independent assessment of your Firm's infrastructure

Development Lifecycle

Review processes of onboarding new or refreshed technologies into your environment and identify risk mitigations that are in place

Incident Response Plan

A well thought-out and thorough incident response plan will ensure swift and effective reaction if an organisation does experience a security incident

Threat Intelligence

Threat intelligence can be used to identify and manage risk; informing strategy. Threats can be prioritized and mitigated improving the overall effectiveness of cyber defenses

Employee Training & Testing

Establish a mandatory baseline training program for all employees that focuses on the upskilling of employees. Once established, it is key to actively update and test them on the latest threat landscape

Third Party Security

Understand your third-party environment and upgrade your contract provisions so that third parties are following the same standards you are striving for in your own environments

Exercises & Drills

Engagements should include participants from across all major lines of business and public-private sector organizations. Each event should result in documented findings with completion timeframes

Least Privilege Access Management

Employees should only have access to the systems and specific information they need to do their jobs. Protective action should be taken when an employee leaves or transfers department

JPMorganChase

Yes, check fraud still exists

In fact, payment by check continues to account for a significant portion of all B2B payments. According to the 2022 AFP Report, **66% of respondents reported falling victim to check fraud**[1]

FIRST HALF OF 2023

305 USPS letter carriers robbed on the job[3]

25K+ incidents of high-volume mail theft reported[3]

"U.S. Postal Service warning users against sending checks through the mail"[2]

Front of Check Fraud	Altered Checks | Criminals alter the name or payment amount before depositing Counterfeit Checks | Criminals use printers and desktop publishing software to create counterfeit checks
Back of Check Fraud	Improper Endorsements | Criminal forges endorsement, or chooses not to endorse at all Mobile Deposit Fraud | Usually perpetrated by the intended recipient, sometimes to double-cash paychecks

[1] 2023 Association for Financial Professionals (AFP) Payments Fraud Survey
[2] 2023 Delano, Jon. "U.S. Postal Service warning users against sending checks through the mail" CBSNews.com, June 20, 2023, https://www.cbsnews.com/pittsburgh/news/u-s-postal-service-warning-checks-mail/
[3] United States Postal Service, USPS, Postal Inspection Service Roll Out Expanded Crime Prevention Measures to Crack Down on Mail Theft, Enhance Employee Safety and Strengthen Consumer Protections, May 12, 2023

What to expect when check fraud happens

1 | Claim is reported

The client informs the bank and reports a claim

2 | Documentation is provided

The client provides the required documentation to Chase

3 | Investigation

Back-of-check fraud

Chase makes a claim on the bank where the check was deposited

- **If deposited at a Chase bank**, it could take up to 15-20 business days if all the required documents have been provided
- **If the bank was not Chase**, it could take six months or more
- We reach out to the other banks with the claim; however, they control the response time frame

Mobile Deposit Fraud

Chase makes a claim on remote deposit capture bank

- **If deposited at a Chase bank**, it could take up to 15-20 business days if all the required documents have been provided
- **If the bank was not Chase**, it could take up to 30 business days
- We reach out to the other bank with the claim; however, they control the response time frame

Front-of-check fraud or counterfeit

- Internal Chase investigation could take up to 15-20 business days if all the required documents have been provided

Other reasons your claim could be delayed

- The depositing bank could ask for more documentation such as W-9 forms, tax documents, police report, driver's license or a payee-signed affidavit.
- The case could also involve an altered check or dual payees

4 | Resolution

The claim is paid or denied. If there is a request for more information, then you must go back to Step 3

Business Email Compromise Trends and Prevention

Trending Scenarios

- **Real Estate Transactions:** During a real estate transaction, criminals may impersonate sellers, realtors, title companies or law firms to trick the home buyer into transferring funds into a fraudulent account.
- **Data and W-2 Theft:** Criminals use a spoofed or compromised executive email account to send fraudulent requests for W-2 information or other personally identifiable information to HR staff or others within the business who maintain confidential employee records.
- **Supply Chain:** Criminals send fraudulent wire transfer requests to redirect funds during a pending business deal, transaction or invoice payment to an account controlled by organized crime groups.
- **Law Firms:** Criminals discover information about pending litigation or trusts and impersonate a law firm's client to change the recipient bank information to a fraudulent account.
- **Construction Projects:** Criminals search the websites of public schools, colleges and universities that promote their construction projects then use that information to pose as the contractor or construction company to divert the funds to the scammer's accounts.
- **Gift Cards:** Criminals use a spoofed or compromised executive email account to send fraudulent requests for gift cards as holiday gifts or performance awards.

Practices To Help Prevent BEC

- Train employees on suspicious email trends
- Enable controls so all emails from outside the firm are marked as external
- Enable email controls:
  - SPF – Sender Policy Framework
  - DKIM – Domain Keys Identified Mail
  - DMARC – Domain-based Message Authentication, Reporting & Conformance
- **Do not** make payment/payment changes solely based on an email or phone call. Use Callback procedures

Case Study – Fictitious Help Desk Deepfake

WHAT HAPPENED: A help desk employee received a call from a high-level executive requesting to change his password. The caller presented the required credentials and passed the voice authentication and proceeded to change the phone number associated with the account. He was then able to reset the account password and gain full control of the account.

HOW?

- The attacker performed initial open-source reconnaissance to target the executive with a spear-phishing email and gain access to the necessary credentials
- The attacker created a deepfake of the executive's voice using publicly available audio
- The Help Desk voice authentication was bypassed due to the accuracy of the deepfake

What are the lessons learned?

- Use multiple forms of authentication and implement tight controls around changing personal information such as phone numbers and passwords
- Do not rely too heavily on voice authentication
- Limit exposure of employee information (specific job details, audio, and video) on external, public facing platforms

Case Study – Elaborate Deepfake Scheme

WHAT HAPPENED: In January of 2020, a branch manager of a bank in Hong Kong received a call from the company director about an acquisition requiring the transfer of $35 million. A lawyer was hired to coordinate the transfers and emailed the branch manager with confirmation of where to send the money. The branch manager wired the 35$ million.

HOW?

- The attacker created deepfake audio to impersonate the Director's voice
- The voice call and emails appeared to be legitimate to the branch manager, who was familiar with the director's voice, so he complied with the request
- The combination of the voice clone and emails led to increased perceived legitimacy

What are the lessons learned?

- Limit exposure of employee information (specific job details, audio, and video) on external, public facing platforms
- Require callbacks and multiple verifications for major transactions
- Educate employees on the threat of deepfakes in their various forms
- Have and encourage a culture of reporting suspicious activity

Forbes.com

Case Study - Fake Invoices

WHAT HAPPENED: Between 2013 and 2015, a man in Lithuania sent several large tech companies approximately $120m in fake invoices from one of their hardware vendors. The companies paid upon receiving these invoices

HOW?

- The criminals leveraged a known vendor and their invoices
- They sent new/altered invoices to the accounts payable department
- The money was wired to new bank accounts in several countries

What are the lessons learned?

- Use callbacks to confirm any new payment information
- The callback should be to a known good phone number to a known contact
- Enable staff to question suspicious activity and have them slow down when it comes to paying invoices
- Train staff to recognize the signs of business email compromise
- Test staff to see if they comply with the training they have received

DOJ -Justice.gov press release 12/19/2019

Case Study - Fictious Billing Scheme

WHAT HAPPENED: Between August 2020 and March 2022, a former tech company employee provided fake vendor information to unwitting subordinates for input into the company's vendor system. Once in the system, she then approved the invoices

HOW?

- The former employee used a position of authority to direct her employees to enable her criminal acts
- Due to their trust (or fear) of the supervisor, they complied
- There was a lack of controls and separation of duties

What are the lessons learned?

- Ensure there is a separation of duties so that toxic pairs are avoided
- Validate all new vendors to ensure a valid contract exists for work performed
- Validate new vendors with callbacks
- Ensure your organization has robust third-party oversight controls
- Have and encourage a culture of reporting suspicious activity

DOJ -Justice.gov press release 7/5/2023

Performing a Proper Callback

1 – Don't rely on inbound calls

Always conduct an outbound call to the party to confirm they are legitimate.

Never ask that a vendor call you to validate payment instructions.

Never use an inbound call to update contact information.

Why? Relying on inbound calls is an invitation for criminals to call you. If a fraudster has taken over a vendor's email, they'd know when you request that partner to call you. An outbound call from your staff to the party removes the risk that an employee falls prey to an enterprising criminal on the other end of the line.

2 – Don't trust the number provided

Always use a known or trusted number for a system of record, and continually update any internal database for improved reference ability.

Never use a phone number provided to you in an email thread, invoice or attached documentation.

Why? Fraudsters will be all too happy to validate the transaction if you call them directly. Train staff to use this system of record repeatedly, as just one deviation from the controls opens the door to fraud.

3 – Do speak with the requestor

Always speak to the party who is personally accountable for the change in instructions.

Never settle for speaking with just any employee of the vendor that's initiated a payment or change.

Why? Fraudsters with email control will exploit messages between parties. Let's say your staff calls an accounting employee at the vendor, who then emails their own CFO for validation. What your staff and the vendor don't know is that cybercriminals have hacked the CFO's email and control it. This would allow fraudsters to circumvent your controls and direct the accounting employee under the presumed guise of the executive.

4 – Don't assume internal controls have been followed

Always confirm controls were executed as intended and none of the above mistakes were made.

Never presume that a callback was performed.

Why? Human error happens; minimize its risk by actively ensuring procedures have been followed exactly as they were laid out.

Personal Cybersecurity Best Practices

Computers and Phones

- Keep devices updated to ensure the most recent security features are installed
- Turn off Bluetooth and Wi-Fi when not in use
- Keep locked with strong passwords
- Rename devices to a non-descript name
- Only download applications from trusted sources

Home Network

- Change default passwords on networking devices
- Disable SSID broadcasting from router settings to hide network name
- Create a separate “guest” network for visitors to use; create additional networks as needed to segment for different uses

Social Engineering

- Take a cautious approach to opening links in messages or emails coming from untrusted/unknown sources
- Be aware of enhanced social engineering abilities resulting from adversary AI use (better grammar, more convincing images, deepfake voice, etc.)

Password and Account Management

- Create strong and complex passwords; store them in a trusted password manager
- Use MFA whenever possible, especially for sensitive accounts
- Use a unique password for each account
- Do not share passwords, especially for sensitive accounts

Privacy

- Investigate privacy settings for different accounts, devices and applications and choose strict options
- Avoid posting personal information on social media/online platforms

Public Wi-Fi

- Always use a VPN when using public networks
- Be cautious of shoulder surfing when in public
- Consider using a mobile hotspot instead