Fraud protection and cybersecurity

Help keep your business safe

Fraud is on the rise in businesses of all sizes. By learning the common methods used by criminals, and how to spot them, you can help protect your business from potentially devastating consequences.

Contents

Fraud risk is a fact

Cyberthreats and fraud risks are real — most businesses have been targeted by some type of fraud, and it can be costly. Bad actors continuously seek to leverage emerging technology and vulnerabilities to carry out malicious activity across the globe.

While no industry is immune from fraud or cybersecurity threats, some are targeted more frequently:

- HEALTHCARE AND PUBLIC HEALTH
- SOCIAL MEDIA / DIGITAL CURRENCY
- CRITICAL INFRASTRUCTURE
- INFORMATION TECHNOLOGY
- FINANCIAL SERVICES
- TRANSPORTATION / TRAVEL
- MANUFACTURING

51%

of companies in a 2022 survey say they experienced fraud in the last two years[1]

2.4MM

The number of fraud reports received by the Federal Trade Commission in 2022[2]

[1] PwC's Global Economic Crime and Fraud Survey 2022

[2] FTC, "FTC crunches the 2022 numbers. See where scammers continue to crunch customers," 2023.

PRO TIP

Check fraud continues to be a problem, especially for business-to-business transactions where checks are frequently used. Consider exploring fraud protection tools and account alerts that may be offered by your bank.

Cyberattacks and your business

Cybercriminals can use many methods to access and manipulate confidential data belonging to you, your business, your employees and your suppliers.

Some of those methods include:

Phishing emails, SMiShing text and vishing calls

Phishing, SMiShing and vishing are fraudulent attempts to gain access to important personal or company data. These messages may appear to have come from a colleague, a legitimate business or even the government.

Ransomware

Ransomware is a complex form of cyberfraud which often involves more than one type of compromise. Criminals use malware and encryption to hold important company data hostage until a ransom is paid.

Business Email Compromise (BEC)

BEC cybercriminals try to obtain the confidential, personal or financial information of clients and vendors by impersonating business partners over email.

Social engineering

Cybercriminals use social engineering to convince unsuspecting employees to reveal personal or company information by pretending to be someone else online.

PRO TIP

If you suspect your business is a victim of fraud, contact your Chase for Business Banker or another trusted advisor immediately.

Phishing, SMiShing and vishing

Learn how to identify these attacks and better protect your business from threats.

Here are some ways to spot attempts to access your data:

Phishing emails

- Vague or suspicious sender names
- A sender address with a misspelled domain
- Urgent or threatening language that demands a quick response
- Attachments that are not what they seem or links to a suspicious site

SMiShing texts

- An unusual message from an unknown number
- Unexpected links in the message
- Numerous typos or strange characters
- Requests for sensitive information via text message

Vishing calls

- The phone number is unfamiliar or shows up as "unknown"
- A live or pre-recorded robocall prompting you for personal information
- Claims to be from a financial institution, your work or the government
- Inability or refusal to verify their identity or provide a call-back number

PRO TIP

Most legitimate organizations won't request sensitive information via email. Never give information such as usernames, passwords or other sensitive personal information.

What to do when you spot these attempts:

Think before you click or respond

If it looks or sounds like any of these attacks, it probably is. Don't click any links, open attachments or call any numbers the sender provided.

Do an email "hover test"

There are two parts to a link:

- The words describing the link (the part you see)
- The URL

Hover your cursor over any link in an email and review the address. If it doesn't match the link displayed or comes from a public domain like @gmail.com, assume it's risky — don't click it.

3.4B

Estimated number of phishing emails sent every day[3]

[3] AAG, "The Latest Phishing Statistics," March 2023.

PRO TIP

If you aren't sure whether a message is legitimate, contact the company's customer service line directly.

Ransomware

Ransomware is malicious, organized and often global. Many ransomware operations function like a business, using malware and encryption to hold important data hostage until a ransom is paid.

25%

Ransomware was involved in 25% of all breaches in 2022[4]

$812,360

Average ransom payment associated with a ransomware attack[4]

$4.5MM

The victim's total average cost of a ransomware attack[4]

34%

34% of all cyber insurance claims were ransomware-related in the first half of 2022[4]

[4] Tech Target, Ransomware trends, statistics and facts, 2023.

How to better protect yourself from ransomware:

- Block spam and suspicious emails with filtering software
- Identify critical systems and assess vulnerabilities
- Develop a plan to strengthen critical systems and determine what resources are needed
- Test your plan
- Conduct regular back-ups to avoid potential data loss
- Segment your network to add another layer of protection
- Update and patch systems and software

236.1MM

The approximate number of ransomware attacks globally in the first half of 2022.[3]

[3] AAG, "The Latest Phishing Statistics," March 2023.

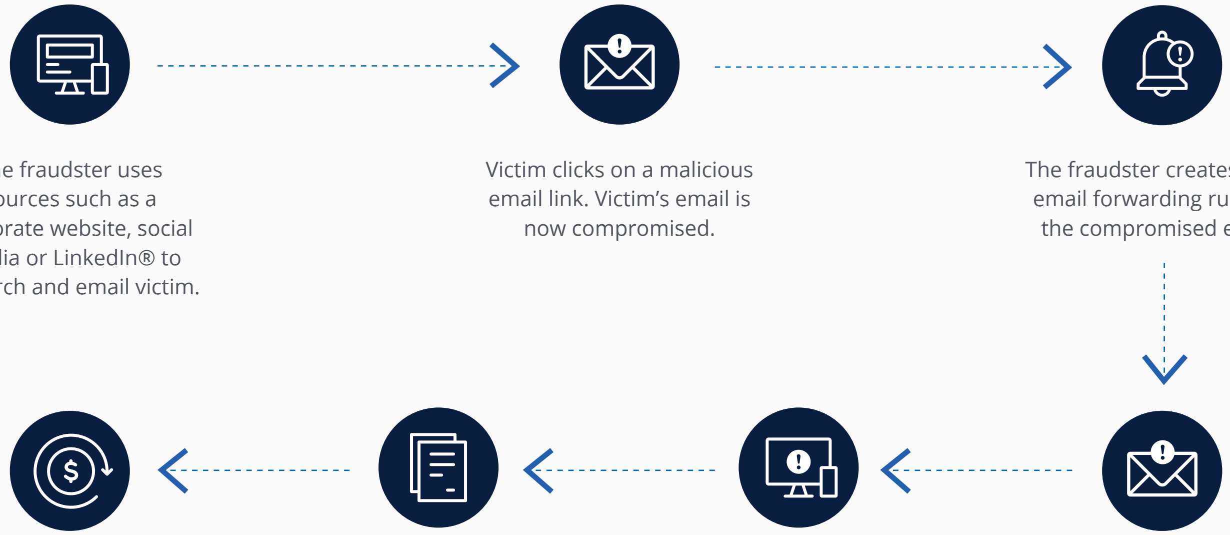
PRO TIP

Immediately reach out to your local FBI field office to report ransomware if you're attacked: **www.fbi.gov/contact-us/field-offices.**

Business Email Compromise (BEC)

BEC cybercriminals impersonate business partners over email in an attempt to obtain confidential, personal or financial information. Businesses reported a total adjusted loss of $2.7 billion due to BEC scams to the FBI in 2022.[5]

BEC in action:



The fraudster uses sources such as a corporate website, social media or LinkedIn® to research and email victim.

Victim clicks on a malicious email link. Victim's email is now compromised.

The fraudster creates inbox email forwarding rules for the compromised email.

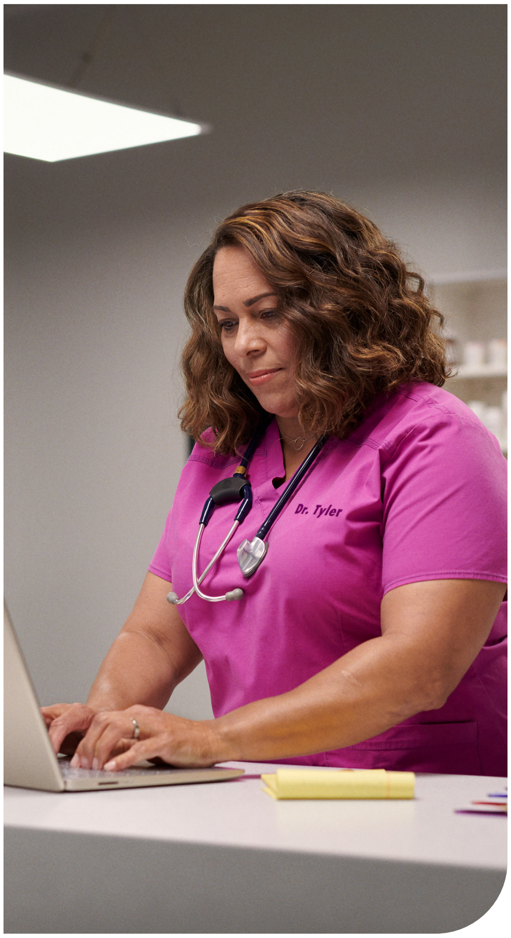
Emails with keywords such as "payment" or "invoice" are automatically forwarded to the fraudster's email.

The fraudster creates a look-alike domain (LAD) to impersonate the victim's legitimate vendor.

The fraudster sends fake invoices out to victim's customers or vendors.

Customers or vendors pay the fake invoices, sending money to a fraudster.

[5] WaterISAC, "FBI 2022 Internet Crime Report"



Signs of a Business Email Compromise attempt:

- Vendors who offer vague reasons for changes to a new account, such as tax audits or current events
- Unsolicited emails, texts, or phone calls to authorize payment requests or change contact information. The individual may insist on digital-only communication
- Requests to conduct activities (such as financial transfers) involving unexpected countries or regions

Pro tips:

Review email security practices

Ask your senior technology leaders about:

- Multifactor authentication to provide extra security that goes beyond usernames and passwords for your customers and vendors
- Automatic labeling of external emails for employees to help prevent the impersonation of trusted vendors and partners

Train employees on BEC prevention

Highlight the importance of callbacks using a phone number that is on file for payment requests and changes to account or contact information.

Test your employees’ BEC knowledge

You can do this regularly by simulating phishing and BEC attempts then sharing results and tips with your employees.

Explore fraud insurance

Contact your insurance agent to discuss fraud insurance options for your business.

Social engineering

Most cyberattacks (up to 98%)[6] rely on social engineering to convince unsuspecting employees to reveal personal or company information. It's important to be able to identify it early and take the necessary steps to stop or prevent it.

Tips to help prevent social engineering:

Confirm

the individual's identity prior to discussing confidential information or taking any requested actions.

Follow

controls for validating new or revised payment information.

Never trust emails, texts or unsolicited phone calls alone to authorize payment requests or change contact information.

Restrict

what information you share on social media such as job title, location or even upcoming travel plans. Fraudsters may use it to target you.

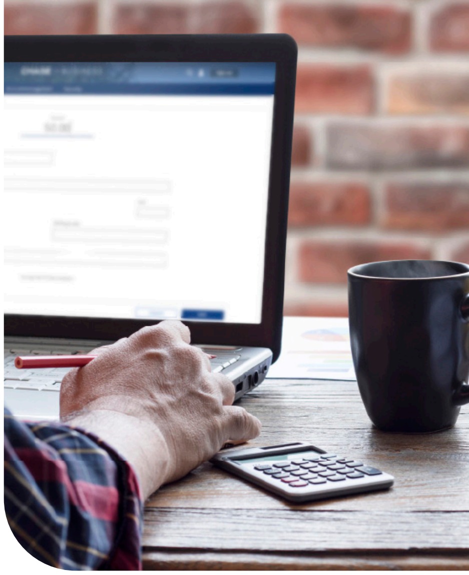
Look for these signs of social engineering:

- Individuals who claim to be a customer, vendor, partner or employee who are asking for information that seems unusual or out of character
- Being contacted by someone who doesn't know you personally and can't confirm their identity upon request
- Attempts to claim authority or status. Social engineers may pose as a senior executive or even a government employee
- Emails or calls that come with urgency or a threat of consequences
- Social engineering can occur in the form of phishing, SMiShing, vishing or even daily conversation

[6] Purplesec Cyber Security Statistics: The Ultimate List Of Stats, Data, & Trends For 2022

PRO TIP

Diligence is key. Train and test all staff regularly against the latest social engineering threats.



Defend your business against fraud

Here are some simple ways to help you protect your business:

01 Keep track of your passwords for all accounts and change them regularly. Always change the default password on your wireless network.

02 Be cautious of clicking on links or attachments sent to you in emails.

03 Turn off Bluetooth® when it's not needed.

04 Keep your screen lock on, choose strong passwords and use biometric tools when available.

05 Create one network for you, another for your employees or guests.

06 Install the latest anti-virus and ad-blocking software.

07 Choose a reputable email provider that offers spam filtering and multi-authentication.

08 Keep all software, browsers and operating systems up to date.

09 Download software only from trusted sources.

10 Never use public Wi-Fi to enter personal credentials on a website. If you must, consider using a VPN.

READY TO GET STARTED?

Contact your Chase Business Banker today to learn more about protecting your business.

CHASE for BUSINESS® | Fraud protection and cybersecurity

For informational/educational purposes only: These views may differ from other employees and departments of JPMorgan Chase & Co. Views and strategies described may not be appropriate for everyone and are not intended as specific advice/recommendation for any individual. You should carefully consider your needs and objectives before making any decisions and consult the appropriate professional(s). Outlooks and past performance are not guarantees of future results.

FOR EDUCATIONAL PURPOSES ONLY