Types of fraud and how they originate

Cybercriminals continue to target online banking and electronic payment transactions. Fraud committed against business bank accounts generally occurs by writing unauthorized checks or through ACH and wire fraud. With two bits of information, your business checking account number and bank routing number, a criminal can make a payment for goods or services either by phone or online.

How fraud originates

The usual starting point for fraud is social engineering, which is the practice of obtaining sensitive information by tricking people into breaking normal security procedures.

Cybercriminals tend to

- **Look for those who divulge passwords or other sensitive financial or personal information**
- **Direct you to a website to download something malicious**
- **Secretly install malicious software on your computer**
- **Ask for remote access to your computer**

Stages of a breach

Severity is measured through seven stages. Each stage provides an opportunity to interrupt the breach.

- Time lag from the initial attack (stage 1) to a full breach (stage 7) varies by incident, but is typically over a period of months.
- Specific defenses are positioned between each of the seven layers to prevent further exploitation.
- The further in the lifecycle that a breach is interrupted, the more expensive it is to remediate.

Stage	Description	Cost
Target identified	"Threat actor" chooses a "target"	
1 Reconnaissance	Harvesting email addresses, conference information, etc.	
2 Weaponization	Coupling exploit with back door into deliverable payload	
3 Delivery	Delivering weaponized bundle to the victim via email, web, USB, etc.	
4 Exploitation	Exploiting a vulnerability to execute code on a victim system	
5 Installation	Installing malware on the assets	
6 Command and control	Command channel for remote manipulation of victim	
7 Actions on objectives	With "hands on keyboard" access intruders accomplish their original goal	
Target breached	"Threat actor" succeeds at breaching the "target"	

Social engineering

What is it?

Social engineering preys on your employees' good intentions. Many forms of online or offline business fraud are based on the concept of social engineering, in which the perpetrator psychologically manipulates an employee into taking action that will ultimately cost your company time and money. A well-meaning employee will naturally respond to a carefully crafted fraudulent request without pausing to consider the fraud risk.

Examples

Social engineering enables attacks, including **phishing, account hijacking** and **business email compromise (BEC).**

Phishing

What is it?

Phishing exploits the public's trust in well-known corporate brand names. By closely mimicking legitimate brands, phishing emails and websites scam individuals into surrendering passwords, as well as financial or personal information. Variations include spear phishing (targeting individuals), vishing (phishing via telephone or a face-to-face encounter) and SMiShing (via SMS text messaging).

How it works

First, the perpetrator sends a fake notice or email message that appears to be from a legitimate, recognizable company, asking the recipient to verify their account or update their information by clicking a link. The link opens an online form or web page that appears genuine—but actually is designed by the cybercriminal to collect personal and sensitive information from gullible users.

Protect against phishing

- Be suspicious of any unsolicited emails, phone calls or text messages with an urgent request for personal or business information, both from known or unknown senders.
- Never click on an embedded link or attachment, or fill out forms asking for financial information in an unsolicited email or SMS text message.
- Mouse over the link and check the URL for validity.
- Ensure that your operating system, security software and any mobile apps are updated.
- Schedule antivirus software to automatically run on a regular basis.
- Never download or install "free" software.
- Don't respond to malicious online advertisements.

Account hijacking

What is it?

Account hijacking is a type of social media engineering where an individual's email account, computer account or any other account associated with a computing device or service is stolen or "hijacked" by a hacker.

How it works

Attackers may hijack hundreds of accounts at once, or target an individual user to gain control of their identity and access confidential information. Cybercriminals can also hijack online accounts, including those used for cloud-based services, or even an entire desktop computer or server.

Protect against hijacking

- Be suspicious of anyone requesting personal or sensitive information.
- Never provide system credentials or any other personal information on an unsolicited inbound call.
- Always verify the identity of an unsolicited caller by insisting on calling him or her back at a trusted number listed for that company.
- Remember that Caller ID is not a foolproof way to verify a caller's identity.

Business Email Compromise (BEC)

What is it?

Companies that make electronic payments to vendors domestically or internationally are particularly at risk for Business Email Compromise (BEC) scams in which an employee unwittingly authorizes a wire transfer or ACH payment to a wrongdoer.

How it works

BEC attackers typically research their victims to target those in position to execute large wire or ACH payments—and often use phishing tactics and/or email hijacking to do their dirty work.

In a common scenario, someone masquerading as the CEO emails the corporate controller with an "urgent" request for a funds transfer to a particular trade account. Or, a "vendor" sends an urgent demand for payment to ensure continued delivery of goods or access to an account.

Protect against BEC

- Be mindful of emails requesting specific and significant fund transfers, especially if a CEO or CFO is on vacation.
- Establish electronic payment instruction policies and procedures, including altering vendor payment instructions using a known contact number.
- If an "urgent" request is received, confirm validity by contacting the requesting person or organization directly via a trusted telephone number.

What are we doing to defend against fraud?

At KeyBank we're committed to protecting our clients and customers. We utilize multiple techniques to help prevent various types of fraud.

We employ an extensive defense with in-depth controls, including fraud and cybertools that create layers of protection. Other tactics include multi-factor authentication in both customer-facing content and the work stream, as well as shifting from prevent to detect policies for heightened anomaly and heuristic detection. Our team regularly enforces data loss prevention rules for platforms such as email, as well as manages user access, executes data discovery and actively blocks and performs takedown services to protect against phishing.

If you suspect you are a victim of fraud or malware, call **Key's Fraud and Disputes Hotline directly at 1-800-433-0124** for analysis of the situation and further direction. Then contact your Relationship Manager to make them aware of the issue.

To learn more, contact your Relationship Manager, or visit **key.com/security.**

KeyBank
Use the red key.®