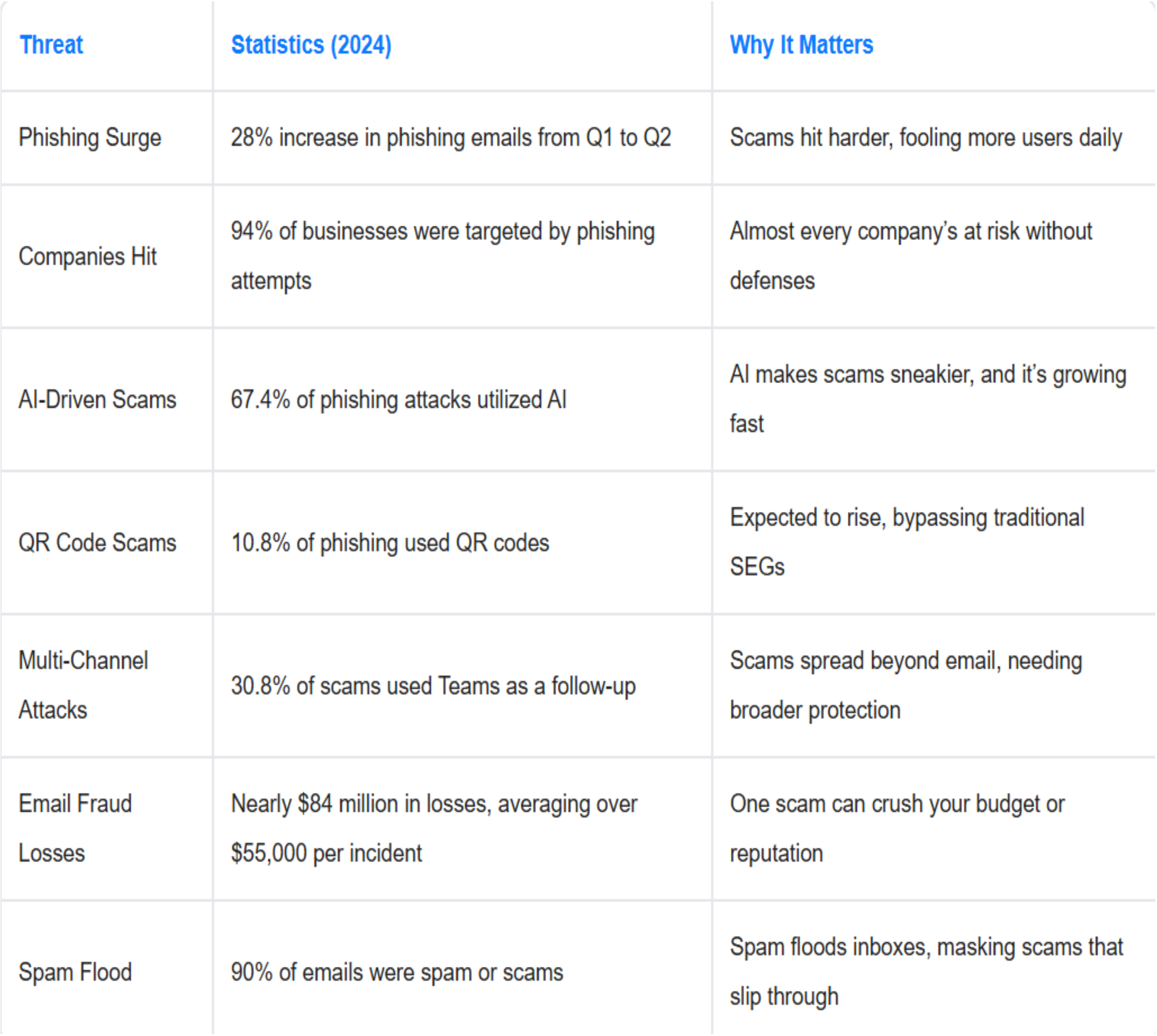
Business Email Compromise (BEC) and Financial Fraud Playbook

The Threat of Deception

Business Email Compromise, or BEC, is a sophisticated social engineering attack that results in financial fraud. Unlike a widespread phishing campaign that tries to capture many credentials, BEC is highly targeted. Attackers impersonate a senior executive, vendor, or trusted business partner to trick an employee, usually in the finance department, into making an unauthorized wire transfer or changing banking details. These attacks directly bypass traditional technical defenses and prey on human trust, demanding an immediate, multidisciplinary response. A statistic by Palisade shows the impact of BEC and Financial Fraud in the current year 2025.



Threat	Statistics (2024)	Why It Matters
Phishing Surge	28% increase in phishing emails from Q1 to Q2	Scams hit harder, fooling more users daily
Companies Hit	94% of businesses were targeted by phishing attempts	Almost every company's at risk without defenses
AI-Driven Scams	67.4% of phishing attacks utilized AI	AI makes scams sneakier, and it's growing fast
QR Code Scams	10.8% of phishing used QR codes	Expected to rise, bypassing traditional SEGs
Multi-Channel Attacks	30.8% of scams used Teams as a follow-up	Scams spread beyond email, needing broader protection
Email Fraud Losses	Nearly $84 million in losses, averaging over $55,000 per incident	One scam can crush your budget or reputation
Spam Flood	90% of emails were spam or scams	Spam floods inboxes, masking scams that slip through

Phase One: Triage and Identification

Speed is essential in this phase because the window to recall fraudulently transferred funds is narrow. The goal is to confirm the compromise and determine the extent of the deception as quickly as possible.

Clear Identification Parameters

1. **Indicators of Compromise (IOCs) in Email:** We look for specific red flags within the email environment. This includes reviewing logs for logins from unusual geographical locations, the use of unfamiliar mail clients, or evidence of brute force attempts prior to the compromise.

2. **Unauthorized Forwarding Rules:** A key indicator of a compromised mailbox is the creation of stealthy, unauthorized forwarding rules. These rules are set up by the attacker to copy all incoming and outgoing messages to an external address, allowing them to monitor conversations and avoid detection after changing a password.

3. **Reviewing Suspicious Requests:** The finance team must be trained to flag requests that violate established procedures, such as a last minute change to a vendor's bank account or an urgent, unverified wire transfer request from an executive to a foreign bank. **Confirming communication authenticity** via an out of band method, like a phone call, is mandatory before any action is taken.

4. **Confirming Financial Impact:** Security must immediately collaborate with the finance and treasury teams to determine if a fraudulent transfer was initiated and, if so, the precise amount and destination bank. This financial triage dictates the urgency of the next phase.

Phase Two: Immediate Containment

Once a BEC incident is confirmed, immediate actions must be taken to stop the attacker's access and prevent further damage.

Containment Strategies

1. **Suspending Compromised Accounts:** The first action is to immediately suspend all access to the compromised email account and any associated cloud resources. This ensures the attacker is locked out of the primary point of entry.

2. **Forced Password Rotation:** All associated credentials for the affected user and any users who recently communicated with them regarding the fraud must be

immediately expired and rotated. New passwords must adhere to high complexity requirements.

3. **Removal of Malicious Forwarding Rules:** Security engineers must manually inspect the mailbox and server level settings to ensure all unauthorized, stealthy forwarding rules are identified and permanently removed. Leaving even one rule allows the attacker to maintain visibility.
4. **Initiating System Isolation:** Depending on the scope of the compromise, we may need to initiate system isolation procedures for the workstation used by the affected employee. This allows forensic imaging of the device while limiting the attacker's ability to pivot to other internal systems.

Phase Three: Fraud Response and Legal Action

This phase focuses on damage control and engaging external parties necessary for recovery and compliance. Time is the most critical factor here.

Coordination and Reporting

1. **Contacting Banking Institutions:** This is the most time sensitive action. The finance and legal teams must immediately contact the sending bank to request a **fraud recall** or a clawback of the wire transfer. The quicker the response, the higher the chance of recovering the funds.
2. **Notifying Law Enforcement:** Legal counsel is responsible for notifying relevant law enforcement agencies, such as the Federal Bureau of Investigation (FBI) in the United States, and filing a formal report. This is often a prerequisite for insurance claims.
3. **Activating Cyber Insurance Policy:** The playbook mandates activating the cyber insurance policy immediately. The insurance provider often has established procedures and preapproved forensic experts who can assist with the investigation and help cover financial losses and response costs.
4. **Stakeholder Coordination:** A command center must be established to ensure continuous, clear communication between Security, Finance, Legal, and Executive Leadership. All major decisions regarding fund recall and public communication must be mutually agreed upon by this core group.

Phase Four: Eradication and Recovery

The incident response team moves to fully remove the threat and prepare the environment for normal operations.

Remediation and Hardening

1. **Forensic Analysis of Mailbox:** A detailed forensic analysis of the compromised mailbox is performed to determine how the attacker gained access and what data they viewed or exfiltrated. This helps identify the original breach vector, whether it was a brute force attack or a session hijacking event.
2. **Restoring Clean Backups:** The compromised mailbox is restored from a clean backup taken prior to the compromise. This ensures any malicious configurations or hidden files left by the attacker are completely eradicated.
3. **Implementing Enhanced MFA:** As a permanent hardening measure, we implement **enhanced multi factor authentication (MFA)** across all affected accounts and potentially expand it across the entire organization. MFA dramatically increases the difficulty for attackers to maintain access even if they steal credentials.
4. **Internal and External Communication:** Based on guidance from Legal and Executive Leadership, appropriate communication templates are used to inform any external vendors or partners whose accounts may have been used or targeted during the deception.

Phase Five: Lessons Learned and Hardening

The final phase ensures the organization learns from the incident and strengthens its defenses against future, similar attacks.

Program Improvement

1. **Reviewing Finance Process Gaps:** The Security and Finance teams jointly review the processes that allowed the fraudulent transfer to occur. Were there adequate checks and balances? Was the separation of duties correctly applied? This ensures **procedural hardening**.
2. **Updating Security Awareness Training:** The incident is converted into a realistic, nonjudgemental case study. We update security awareness training with **real life examples** of the deceptive emails used, focusing specifically on the red flags for wire transfer requests.
3. **Hardening Email Gateway Rules:** Email engineers review and harden gateway rules to prevent similar spoofing attempts, specifically focusing on enforcing sender policy framework (SPF), domain keys identified mail (DKIM), and domain based message authentication, reporting, and conformance (DMARC) policies.
4. **Creating a BEC Checklist:** A concise, easy to use BEC checklist is provided to all employees in the Finance, HR, and Executive Assistant roles, giving them a clear guide on what steps to take if they receive a suspicious, high value request.

This structured approach ensures that our organization can rapidly contain, recover from, and learn from highly deceptive BEC attacks.