

BUSINESS EMAIL COMPROMISE (BEC) & EMAIL SECURITY.



A single convincing email can move money or credentials out the door — **BEC succeeds by impersonating trust, not by breaking encryption or planting malware.**

- DISPLAY NAME SPOOFING
- INVOICE & PAYMENT FRAUD
- SPF / DKIM / DMARC
- ACCOUNT TAKEOVER

01 THE MECHANISM

Impersonation & Pretext

Attackers spoof a display name, a lookalike domain, or use a genuinely compromised account to appear as an executive or vendor, **creating urgency to bypass normal scrutiny.**

Authentication Gaps

Email is only as trustworthy as SPF, DKIM, and DMARC make it — without enforced alignment, **a spoofed sender can land in an inbox looking completely legitimate.**

Payment & Data Redirection

The email itself does no damage; the compromise happens when **a human wires funds, changes banking details, or sends credentials** in response to the pretext.

02 THE FLOW

The Verified Request VERIFIED

- A request to change payment details or move funds arrives by email, apparently from a known vendor or executive.
- The recipient confirms the request out-of-band, using a phone number or contact method not supplied in the email itself.
- Because verification happens outside the email channel, **a spoofed or compromised message cannot complete the fraud** even if it looks convincing.

The Unverified Request DEFRAUDED

- A request to change payment details or move funds arrives, appearing to come from a known vendor or executive.
- The recipient acts on the email alone, trusting the display name and tone without confirming through a separate channel.
- Funds move to an attacker-controlled account, and **by the time the fraud is discovered, the money is typically unrecoverable.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Sender Authentication (SPF/DKIM/DMARC)	Cryptographically verifies that a message actually originated from the domain it claims, and enforces what happens when it doesn't.
Display Name & Domain Monitoring	Detects lookalike domains and spoofed display names impersonating the organization or its executives before they reach a target.
Out-of-Band Verification Process	Requires a second, independent channel to confirm any payment change or unusual request, regardless of how legitimate the email appears.
Account Takeover Detection	Monitors for impossible travel, new mail rules, and other signs a mailbox itself — not just an external sender — has been compromised.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Spam Filtering Alone	No	Catches bulk phishing but misses low-volume, highly targeted BEC messages with no malicious links or attachments.
SPF or DKIM Without DMARC Enforcement	No	Authenticates some legitimate mail but doesn't reject or quarantine messages that fail alignment.
Employee Vigilance Alone	No	Relies on catching a well-researched pretext under time pressure — the exact condition BEC is designed to exploit.
Email Authentication Without Payment Verification	No	Confirms the message's sender but not whether the payment request itself is legitimate.
DMARC Enforcement + Domain Monitoring + Mandatory Out-of-Band Verification	Yes	Blocks spoofed mail at the gateway and stops the fraud even if a message gets through.

BUSINESS EMAIL COMPROMISE.

SPOOF · VERIFY · REDIRECT

05 PROGRAM OPERATIONS

BEC doesn't require malware, so most technical controls never see it.

The email itself is often just well-written text — the fraud happens in the human response, not in an attachment.

DMARC is only protective in enforcement mode.

A policy set to monitor-only reports spoofing attempts without blocking a single one.

Compromised vendor accounts are as dangerous as spoofed ones.

A request from a genuinely hacked supplier mailbox passes every authentication check because it is authentic.

Recovery windows are measured in hours, not days.

Once a fraudulent wire clears international transfer, the odds of recovering funds drop sharply.

06 CONTROL MAPPING

FBI IC3 BEC GUIDANCE

Federal reporting and recovery guidance for business email compromise incidents, including the time-critical fund recovery process.

NIST SP 800-177

Trustworthy email guidelines covering SPF, DKIM, and DMARC deployment for federal systems.

DMARC.ORG (RFC 7489)

The technical standard defining how domain owners publish and enforce sender authentication policy.

FFIEC BANKING GUIDANCE

Wire transfer verification expectations for financial institutions handling payment change requests.

07 WHAT THIS DOES NOT SOLVE

Compromised Vendor Mailboxes

Authentication controls verify a message came from the claimed domain, **not that the account sending it hasn't been taken over.**

Voice & Deepfake Pretexting

Email controls do nothing once an attacker **moves the pretext to a phone call or synthetic voice message.**

Insider-Initiated Fraud

A legitimate employee misusing real access to redirect payments **bypasses every external authentication and monitoring control.**

Cross-Border Recovery

Even a well-detected fraudulent wire can be **unrecoverable once funds clear through international banking corridors.**

08 MYTHS VS. REALITY

MYTH "BEC is just phishing with better grammar."	REALITY BEC often contains no links, attachments, or malware at all — it's frequently indistinguishable from a normal business email until the payment details are checked.
MYTH "SPF and DKIM are enough to stop spoofing."	REALITY Without DMARC enforcing alignment between them, a message can still spoof a domain and pass individual checks.
MYTH "Executives are the only targets."	REALITY Accounts payable, HR, and procurement staff are targeted just as often, since they can directly move money or data.
MYTH "If the account isn't hacked, the email is safe."	REALITY A convincingly spoofed domain or display name requires no account compromise at all.
MYTH "Recovering a fraudulent wire is just a bank problem."	REALITY Recovery depends on reporting within hours through the correct channel — by the time it's "a bank problem," the window has often closed.

09 SPEAK THE PROGRAM — KEY TERMS

SPF (SENDER POLICY FRAMEWORK)

A DNS record listing **which mail servers are authorized** to send email for a domain.

DKIM (DOMAINKEYS IDENTIFIED MAIL)

A cryptographic signature on outgoing mail that **proves it wasn't altered in transit** and came from an authorized source.

DMARC

A policy layered on SPF and DKIM that tells receiving servers **what to do with a message that fails both**, and reports back on spoofing attempts.

DISPLAY NAME SPOOFING

Forging the human-readable "From" name shown in an inbox, while the **underlying email address may be unrelated or lookalike.**

VENDOR EMAIL COMPROMISE (VEC)

A BEC variant where an attacker uses a **genuinely compromised supplier mailbox** to redirect payments from its real customers.

OUT-OF-BAND VERIFICATION

Confirming a request through a separate communication channel, such as a phone call to a known number, **before acting on it.**