



How Business Email Compromise Leads to Financial Loss and How to Stop It

Local governments conduct a tremendous amount of business through email. Invoices are received, vendors are contacted, payment information is exchanged, and approvals are communicated every day.

That convenience also creates an opportunity for cybercriminals.

Business Email Compromise (BEC) is a targeted form of fraud in which a criminal impersonates a trusted vendor, executive, employee, or other contact to convince an organization to send money or change payment information. Unlike many cyberattacks, BEC does not necessarily rely on sophisticated technology or malware.

Instead, it exploits something every organization depends on. Trust.

How a BEC Attack Happens

BEC attacks are often carefully planned.

Criminals may begin by researching an organization and its vendors. Local governments make significant amounts of information publicly available, including staff names, organizational charts, meeting documents, contracts, purchasing information, and vendor awards. Attackers can use this information to identify employees involved in finance, accounts payable, procurement, or executive decision-making.

The criminal may then compromise a legitimate email account through phishing or stolen credentials. In other cases, the attacker creates a convincing lookalike email address, sometimes changing only a single letter or character.

Once positioned inside or alongside a legitimate email conversation, the attacker may wait for the right opportunity. They learn how employees communicate, who handles payments, which vendors are involved, and when money is expected to move.

Then comes the fraudulent request.

An employee may receive what appears to be a routine message from a familiar vendor:

“Please update our banking information for future payments.”

The message may even appear within an existing email conversation. The vendor is familiar. The invoice is real. The payment is expected. Nothing immediately looks suspicious.

That is precisely why these attacks are so effective.

If the organization changes the banking information and sends the payment, the money goes to an account controlled by the criminal. Those funds may then be quickly moved through additional accounts, making recovery extremely difficult.



The Most Important Control: Verify

The good news is that BEC is also one of the most preventable forms of cyber-related financial loss.

The most important rule is simple:

Never change payment or banking information based on an email request alone.

Any request to establish or change banking information should be independently verified using contact information the organization already knows to be legitimate.

Pick up the phone and call a known vendor contact using a verified telephone number already on file.

Do not use the telephone number provided in the change request. Do not rely on a new contact identified in the email. And do not simply reply to the same email asking whether the request is legitimate. If an attacker controls the email account, you may simply be asking the criminal to confirm their own fraudulent request.

A two-minute telephone call can prevent a significant financial loss.

Build Safeguards into the Process

Verification works best when it is part of a formal process rather than something employees are expected to remember when an unusual request arrives.

Vendor banking changes should be treated as **high-risk transactions**. Organizations should consider requiring standardized change forms, supporting documentation, independent verification, and appropriate authorization before making changes.

Whenever possible, responsibilities should also be separated. One employee might enter a vendor change, another approves it, and another release the payment. Multiple levels of review make it much more difficult for one compromised account or one mistake to result in a financial loss.

Organizations should also consider a mandatory delay for the first payment following a banking change, particularly when a request is urgent or occurs immediately before a scheduled payment. Vendors can be informed in advance that banking changes automatically trigger additional verification and may delay payment.

Slowing down the process is not inefficiency. It is protection.

Technology Helps, but It Isn't Enough

Technical safeguards remain important. Multi-factor authentication (MFA), phishing protections, email security tools, and external email warnings can reduce risk.

But technology alone cannot eliminate BEC.

An employee may receive a legitimate-looking request from an actual compromised vendor account. There may be no suspicious attachment, malicious link, or obvious warning for security software to detect.



That is why strong financial procedures provide such an important final layer of defense.

Make Verification Part of Your Culture

Employees involved in financial transactions should be trained to recognize situations commonly associated with BEC, including vendor banking changes, employee direct-deposit changes, executive requests for urgent payments, unusual wire instructions, and subtle changes to email addresses.

Most importantly, employees must be empowered to question a request, even when it appears to come from an executive, longtime vendor, or other trusted person.

Employees should feel comfortable saying:

“I need to independently verify this before I can process the request, and that verification may result in a delay.”

Leadership should support that response. Urgency and convenience should never override established financial controls.

BEC succeeds when **trust is exploited and urgency overrides process**. It works because the request looks routine.

The defense can be equally simple:

Slow down. Verify. Approve.

1. Slow Down

Treat every request to change vendor banking or payment information as high risk - even if the email appears legitimate or comes from a known contact.

2. VERIFY

Pick up the phone. Call a known vendor contact using a trusted number already on file. Never use the phone number provided in the change request or rely on email alone for verification.

3. Approve

Follow your organization’s established approval process before making the change. Whenever possible, require a second person to review and approve the change before funds are released.

When it comes to financial transactions, **email is a method of communication - not proof of authority.**

If your organization would like assistance educating employees about Business Email Compromise or strengthening procedures designed to prevent fraudulent payments, reach out to the **Cyber Squad**. We’re here to help you stay one step ahead.

Remember: Cyber risk is human risk.