



Mail Server Solution

Website
www.sharetech.com.tw/en-us

Sales Info
sales@sharetech.com.tw

Tech Support
help@sharetech.com.tw



"BEC is one of the most financially damaging online crimes," says the FBI.

As digital transformation accelerates and AI becomes widespread, cyberattacks are evolving beyond technical breaches to exploit human trust. From ransomware and supply chain incidents to credential leaks and deepfake scams, it's clear that cybersecurity threats have shifted from technical breaches to psychological manipulation.

While many companies have deployed antivirus and EDR solutions, the FBI Internet Crime Complaint Center (IC3) reports that Business Email Compromise (BEC) remains one of the most financially damaging cyberattacks. With generative AI and deepfake tools, scammers can now craft convincing emails that mimic executives, fake websites, and real-time payment instructions, making traditional defenses ineffective. Without intelligent email analysis and identity verification, a single fraudulent email can cost a company millions and its reputation.

What is BEC?

According to the FBI Internet Crime Complaint Center's Internet Crime Report 2024:

"BEC is a scam targeting businesses or individuals working with suppliers and/or businesses regularly performing wire transfer payments. These sophisticated scams are carried out by fraudsters by compromising email accounts and other forms of communication such as phone numbers and virtual meeting applications, through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds."

(Source: [FBI Internet Crime Complaint Center, Internet Crime Report 2024, p. 12](#))



1

Identify Targets

Focus on finance staff or executives.



3

Steal Credentials

Obtain email passwords and wait to strike.



2

Social Engineering Attack

Use phishing or virus.



4

Execute BEC Scam

Impersonate vendors or finance personnel to defraud.

Four reasons BEC keeps succeeding

1. Social engineering traps

Attackers impersonate executives, suppliers, or partners with urgent, convincing messages to trick victims into transferring funds or revealing sensitive information.

2. Low-volume emails

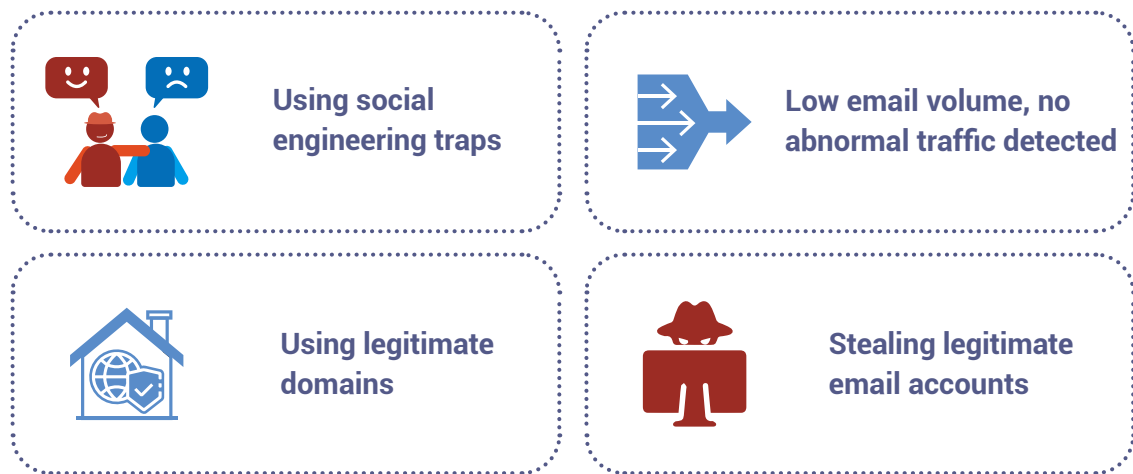
BEC uses precise, targeted sends rather than mass-mailing, so it doesn't trigger traffic anomalies or spam filters and often evades automated detection.

3. Legitimate-looking domains

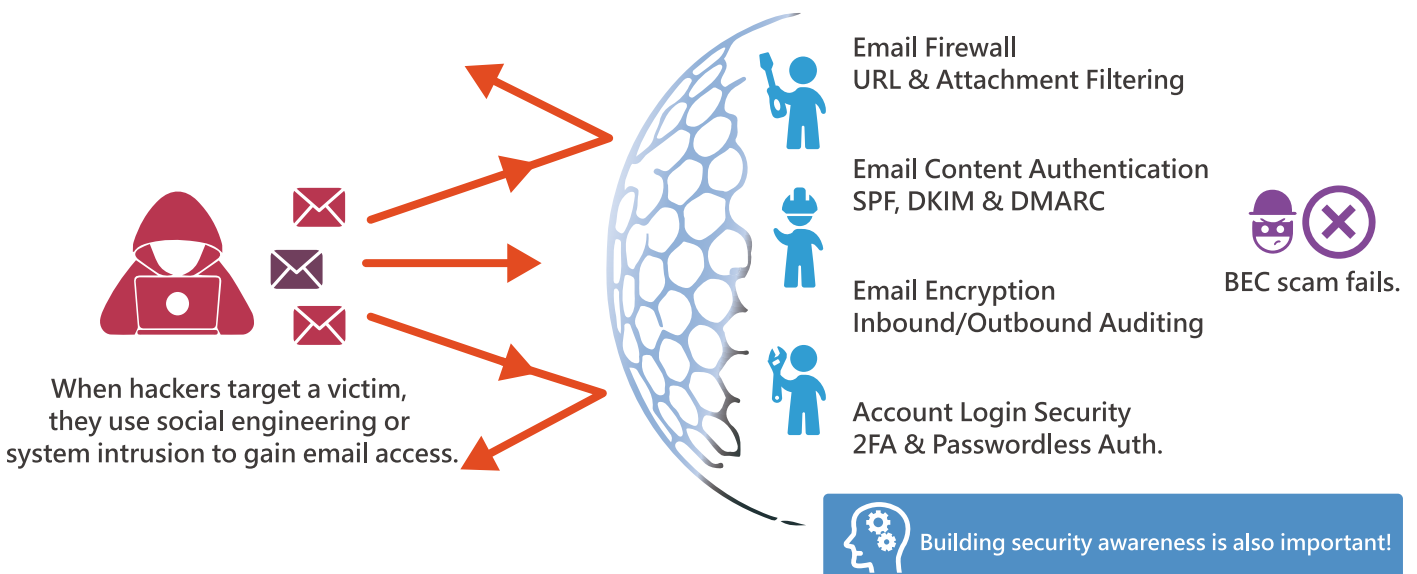
Attackers register look-alike domains and mimic brand elements (logos, signatures, templates) to make messages appear authentic.

4. Compromise of legitimate email accounts

Once an internal account is hijacked, they can send emails from a legitimate address, making it difficult for both security systems and recipients to recognize the fraud.



ShareTech's Four Lines of Defense Against BEC Attacks



1st Line of Defense – Email Firewall, URL & Attachment Filtering

ShareTech strengthens email security through **abnormal sending detection**, **SMTP SASL**, **abnormal user authentication**, and **reply-abnormal sender verification**, filtering threats that traditional firewalls miss.






- **Abnormal Sending Detection:** If an email's subject or attachment name matches predefined conditions, it's quarantined automatically. Receiving multiple identical emails at once also triggers quarantine or sender IP blocking.
- **SMTP SASL:** When the SMTP login account and sender name don't match, the system blocks the sender's IP for a period to prevent impersonation.
- **Abnormal User Authentication:** The system monitors SMTP(S), POP3(S), and IMAP(S) login activities, stopping attempts to brute-force passwords.
- **Reply - Abnormal Sender Verification:** When enabled, the system flags new reply senders or IPs by adding a warning tag to the subject.

Additionally, ShareTech's built-in **URL database**  **URL** blocks malicious links, while **Sandstorm advanced malware filtering**  detects and isolates unknown threats hidden in common attachments such as docx, xlsx, pptx, or pdf files—providing multilayered content protection.


2nd Line of Defense – Email Content Authentication, SPF, DKIM & DMARC


ShareTech provides **signature verification**, allowing recipients to verify message authenticity through a link that confirms it directly with the sender's mail server, reducing the risk of tampering.



 <p>SPF</p>	 <p>DKIM</p>	 <p>DMARC</p>
<p>SPF prevents forged emails sent from unauthorized servers</p>	<p>DKIM ensures message integrity by confirming that the email content has not been altered in transit</p>	<p>DMARC instructs the receiving server on how to handle messages that fail SPF or DKIM checks—whether to accept, quarantine, or reject them. It can also send reports back to the sender, allowing organizations to see if anyone is impersonating their domain.</p>

3rd Line of Defense – Email Encryption & Inbound/Outbound Auditing

Even if an email account is compromised, the **automatic encryption**  of important messages and attachments prevents unauthorized users from accessing their content.

ShareTech also **audits keywords in subjects and message bodies for both incoming and outgoing emails** , applying actions such as quarantine, deletion, notification, or copy forwarding to prevent confidential data leak.

4th Line of Defense – Account Login Security

To prevent employees from using weak passwords, the admin can enforce password rules—requiring uppercase letters, symbols, and minimum length. Users can also enable **two-factor authentication (2FA)** via Google Authenticator or email verification. The system also sends alerts for suspicious logins to keep accounts secure.

Account

sharetech

Password

FAt19er3@! |

Enter

Email verify

google authenticator
verify



ShareTech further offers a **passwordless authentication app** that supports fingerprint or facial recognition for quick, secure logins.

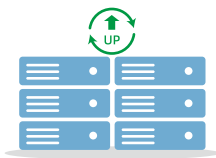


ShareTech partners with **GoTrust for FIDO-standard authentication** using biometrics or security keys, providing stronger, multi-layered protection.

Invisible Defense – Building Cybersecurity Awareness

The key feature of BEC scams lies in exploiting people's trust in email communication. Many employees act on messages without verifying the sender, giving attackers a way in. Building awareness from simple habits—**avoiding suspicious links, updating passwords, and enabling multi-factor authentication**—is vital.

ShareTech goes beyond education by offering **social engineering drills** that train employees to detect and respond to real BEC threats.



To counter evolving threats, ShareTech provides **regular system updates** to ensure timely protection. With 20+ years of email security expertise, ShareTech has been helping organizations strengthen defense from system to human level.