An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2507120126

NCSC Guidance

Protecting Against Business Email Compromise and Payment Fraud

25 July 2025

STATUS: TLP: CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration

What is BEC?

Business Email Compromise (BEC) is a type of cybercrime where attackers impersonate a legitimate business contact - often a company executive, supplier, or employee - to trick individuals into transferring money or sensitive data. It typically involves email fraud and social engineering, and it can cause significant financial and reputational damage.

Common BEC scenarios include:

- **CEO fraud**: An attacker pretends to be a company executive requesting an urgent wire transfer.
- **Supplier fraud**: A vendor's email is compromised and used to send fake invoices or change payment details.
- **Payroll diversion**: Attackers trick HR or payroll staff into changing an employee's direct deposit account.
- **Legal representative impersonation**: Criminals pose as legal counsel to pressure action on a confidential matter.

Real-World Examples

Business Email Compromise (BEC) costs Irish organisations millions every year. In 2023, SMEs alone lost almost €10m to invoice redirect fraud. Organisations of all sizes are vulnerable to this type of attack, which mainly focusses on payment fraud by impersonating trusted contacts such as suppliers, executives, or partners.

Public Sector Case (Ireland, 2023): A local authority paid over €500,000 to a fraudster after receiving a fake invoice from a spoofed supplier email address. The email appeared credible, and payment was made without secondary verification. The loss was not recoverable.

Private Company Case (Ireland, 2022): A private company had over €98,000 stolen as a result of a BEC fraud. The money was transferred to a bank a/c in Portugal - working with the financial institution, the payment was cancelled, and all the money was recovered.

EU Manufacturer (Germany, 2016): A finance executive wired €40 million based on spoofed emails and phone calls claiming to be from their CEO and legal counsel. The attackers had studied the company's leadership and operations extensively beforehand.

An Roinn Dlí agus Cirt, Gnóthaí
Baile agus Imirce
Department of Justice,
Home Affairs and Migration

How to Recognise a BEC Attempt

Look out for:

- Unexpected payment requests or changes to payment instructions.
- Emails from executives or vendors requesting urgent action or confidentiality.
- Slightly altered email addresses or domain names.
- Unusual language, grammar mistakes, or inconsistent formatting in emails.
- Messages asking you to bypass normal processes or send sensitive info.
- Example Warning Signs:
  - "Can you wire this immediately? I'm in a meeting and can't talk."
  - Please update my direct deposit details before the next payroll."

How BEC Works: The Attack Lifecycle

To effectively prevent BEC, it helps to understand how attackers operate. Each stage offers opportunities to detect or disrupt the attack.

Tom Johnson House, Beggar's Bush, Dublin 4, Ireland, D04 K7X4
T +353 (0)1 678 2333 E info@ncsc.gov.ie
ncsc.gov.ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

1. Reconnaissance

What attackers do:

Gather open-source intelligence (OSINT) on staff roles, supplier relationships, and payment schedules (e.g. via LinkedIn, company websites, breached data).

What you can do:

- Limit public availability of organisational charts and contact information.
- Train staff to be cautious about posting work-related details online.
- Watch for domain look-alikes or typo squat registrations.
- Maintain an up-to-date supplier list with verified contact points.

Attackers often know the names of your finance staff before they send a single email.

---

2. Initial Access / Spoofing

What attackers do:

Use compromised accounts, spoofed email addresses, or registered lookalike domains to impersonate trusted individuals or organisations.

What you can do:

- Enforce Multi-Factor Authentication (MFA) on all email accounts.
- Implement and monitor SPF, DKIM, and DMARC on your domains.
- Block inbound email from newly registered domains or domains with small typos.
- Use anti-spoofing and email filtering tools to flag anomalies.

---

*Most BEC attacks do **not** involve malware - traditional antivirus won't catch them.*

---

3. Social Engineering / Deception

What attackers do:

Craft convincing messages urging finance or procurement staff to take urgent action—typically to change bank details or make a payment.

What you can do:

- Use a strict call-back verification process for any change in bank details.

- Require dual approval for financial transactions over a set threshold.
- Train staff to spot red flags: urgency, secrecy, external domains, unusual tone.

A "quick update to bank details" should always trigger a phone call.

---

4. Execution / Funds Transfer

What attackers do:
Trick your team into sending funds to accounts under criminal control.

What you can do:

- Delay large payments by default to allow for fraud detection.
- Use payment-processing software that flags unusual changes in payee data.
- Keep payment platforms isolated from email systems where possible.

5. Post-Event Actions

What attackers do:
Fraudsters act fast — stolen funds are often moved quickly through money mule accounts and overseas banks, making recovery extremely difficult.

What you can do:
Act Immediately

- Stop the payment if possible. Contact your bank to halt or reverse the transaction.
- Notify your organisation's IT or security team without delay.
- Escalate to your bank's fraud team — having a pre-established relationship can speed up response.

Report the Incident

- An Garda Síochána – https://www.garda.ie/en/contact-us/
- National Cyber Security Centre (NCSC) – https://www.ncsc.gov.ie/contact/
- Notify affected parties (e.g. customers, vendors) if their data or payments may be at risk.

Preserve Evidence

- Do not delete any emails or communications involved.

- Save email headers, logs, call recordings, and transaction details — these are vital for investigation and potential recovery.

Review and Strengthen Security

- Change compromised passwords and check for suspicious email forwarding rules.
- Assess how the attacker succeeded and update internal policies, controls, or staff training accordingly.
- Test and refine your incident response plan regularly to ensure readiness.

Most funds are unrecoverable if not flagged within the first few hours.

Important Note: To mitigate BEC and a wide range of cyber threats the NCSC recommend organisations implement a comprehensive cyber security standard, such as the Cyber Fundamentals Framework™ (CyFun). The controls mentioned above have been mapped to the relevant CyFun clauses in Annex A of this document.

Summary Checklist

Do	Don't
Use MFA	Trust emails or calls based on name alone
Verify payment changes by phone (using known contacts	Assume a call is genuine just because the voice sounds familiar
Train staff to spot BEC and vishing tactics	Be rushed into acting under pressure
Report incidents quickly	Feel embarrassed about falling for a scam

Further Reading

- FraudSmart: Fraud & Scams - FraudSMART
- An Garda Síochána: An Garda Síochána warn employees about fraudulent email payment requests - Garda

ANNEX A: Mapping to Cyber Fundamentals Framework

The following controls of the CyFun Framework will prevent or mitigate Business Email Compromise (BEC) and payment fraud attacks.

Control Area	Relevant CyFun Clause	Description
Asset Management	ID.AM-1, ID.AM-2	Maintain inventories of hardware and software, including email systems and payment platforms
Access Control	PR.AC-3, PR.AC-4	Use MFA for remote access; enforce least privilege and separation of duties in finance
Awareness & Training	PR.AT-1	Staff are trained in identifying phishing and social engineering
Information Protection	PR.IP-4	Backups conducted, maintained and tested (for email and finance systems)
Protective Technology	PR.PT-4	SPF/DKIM/DMARC; email/web filtering; block unauthorised forwarding
Maintenance	PR.MA-1	Ensure mail servers and endpoints are patched and maintained
Anomalies & Events	DE.AE-3	Collect and review event logs from email and finance platforms
Security Continuous Monitoring	DE.CM-1, DE.CM-3	Monitor user and network activity, including forwarding rules
Response Planning	RS.RP-1	Maintain and test incident response plans
Improvements	RS.IM-1	Incorporate lessons learned after incidents
Recovery Planning	RC.RP-1	Have a documented and tested recovery plan, especially for financial systems

Note: The mapping is aligned to the "Basic" assurance level as defined in the Cyber Fundamentals Framework (v2024.1).