# Business Email Compromise (BEC) Quick Facts

- **23,775** Number of Business Email Compromise (BEC) Phishing E-mails in 2019
- **$1,776,549,688** Financial Loss
- **$100 M** Cost of an attack

## What is Business Email Compromise?

Business email phishing and domain spoofing tactics to compromise a legitimate business email account and execute fraudulent activities. With origins in CEO or executive impersonation, BEC has now expanded in scope to include personal emails and external vendor email.

## How to Recognize a BEC Attack?

BEC attacks are very targeted and well-executed, making it difficult to differentiate these from legitimate emails. Here are some red flags to look for:

- **"Urgent" or "Immediate" vendor request payment**
- **Vendor payment request from a new email or with new bank account/routing number**
- **Request for payments before the weekend or holidays**
- **Request for wire transfer or personal account**
- **Email from a spoofed C-level executive**

All of these emails target the people of the human layer—something most anti-phishing tools ignore.

Recognizing and preventing BEC attacks requires creation of a baseline for communication patterns and conversation styles to identify anomalies and a strong security awareness education program in place.

## Learn How to Stop BEC Attacks with Tessian.

With Tessian’s Human Layer Security platform, you can detect sophisticated and targeted BEC attacks in real-time and ensure that your employees learn to recognize such attacks with our non-disruptive and in-the-moment alerts.