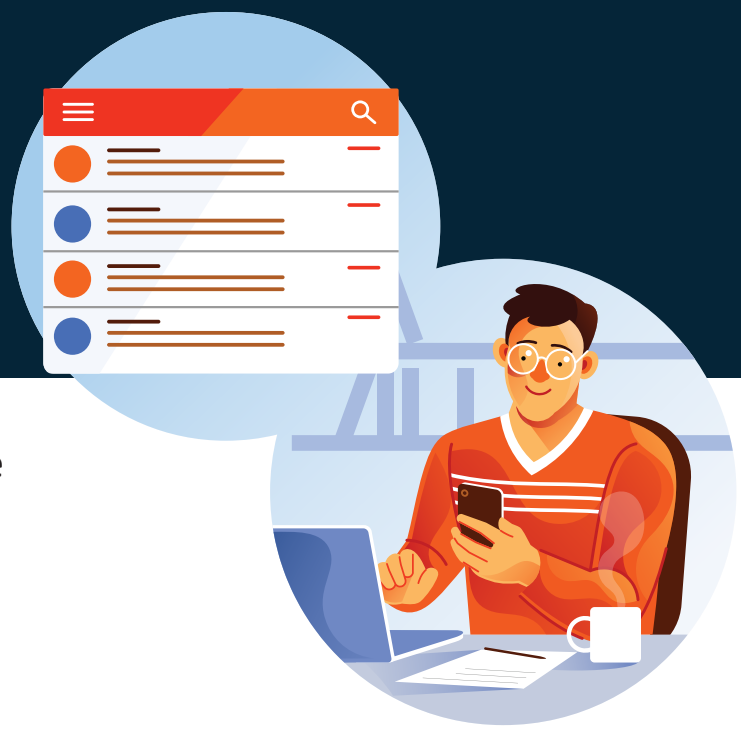
BEC Taxonomy:
Let's Simplify It

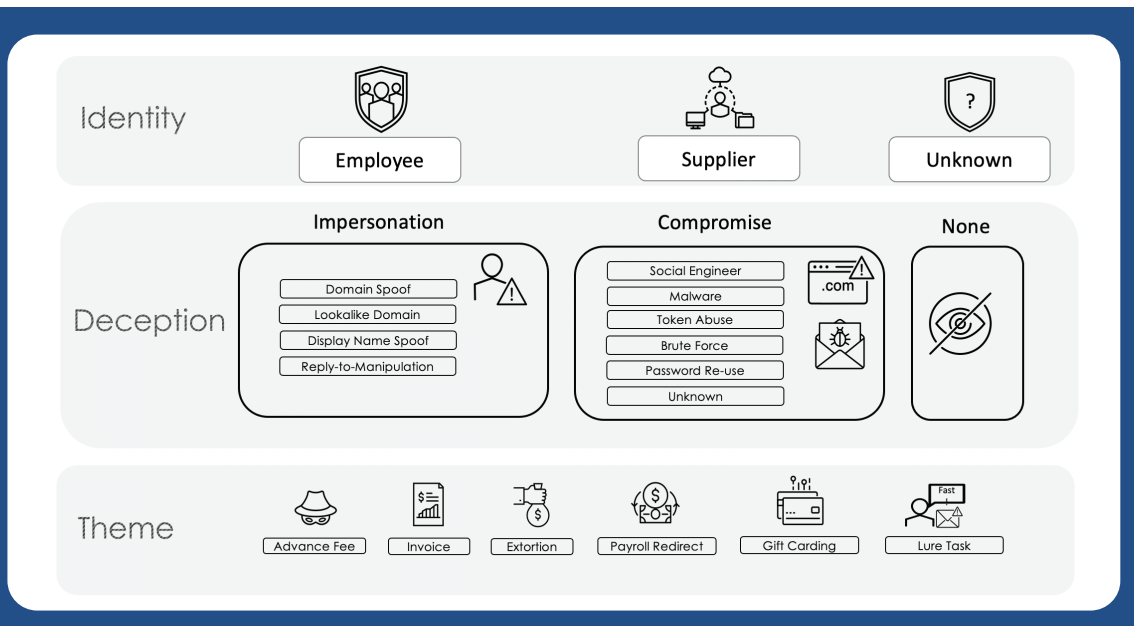


Business Email Compromise (BEC) is a type of email fraud. It is one of the most financially damaging threats to businesses of all sizes and across all industries. However, as BEC schemes have evolved, the terms used to explain it have become confusing. There is a lot of unnecessary blending and blurring of information, causing terms to become misused.

The problem is that BEC is often used as a sweeping, generalized term, describing an entire subclassification of email threats. When people use the term, they are usually referring to attacks that use one or more techniques associated with financially motivated, response-based, socially engineered email deception. What a mouthful! That's why BEC has now become too inclusive to be useful in research and customer prioritization of threat risks and exposure. But don't worry, we're here to help!

Email Fraud Taxonomy

This Email Fraud Taxonomy map helps to simplify and specify the important aspects of BEC. The map helps make it manageable for organizations and researchers to label and understand the specific email fraud facing them.



Identity

In this top tier, "Identity" refers to who the threat actor is pretending to be. An organization can make this level more detailed to better fit their needs by adjusting the categories. For instance, they can expand "Employee" into two categories: "Executives" and "General Employees."

Deception

The following tier, "Deception," is a grouping of techniques used by email fraud threat actors. These techniques include:

- **Impersonation** – An attack in which the threat actor manipulates one or more message headers to mask the origin of the message.
- **Compromise** – An attack in which a threat actor gains access to a legitimate mailbox.

The "None" category refers to instances when other tactics are used, such as those requiring no impersonation, or in which fraudulent emails are sent from free email providers with no spoofing.

Theme

The final tier, "Theme," is the most important part of this taxonomy. That's because the most relatable and actionable information is typically derived from this tier.

The themes included are constructed to represent categories that are relevant to the BEC threat landscape and resonate with most businesses. By design, they are generic enough to account for nuance, yet specific enough for rapid manual identification purposes.

Follow These Tips!

- Always verify that an email sender is who they say they are. If you recognize the sender but notice their email is slightly different, report it.
- Be on the lookout for the deceptive techniques identified in this BEC taxonomy map.
- Threat actors rely heavily on "theme" during BEC attacks. Be wary of anything that urges you to take quick action.

By using this BEC Taxonomy map, you can help your organization and end users avoid these attacks and become better at cybersecurity awareness.