What Is Business Email Compromise and Should I Be Concerned?

Did you know that email is the starting point for 91% of cyberattacks?*

According to the FBI's 2022 Congressional Report, business email compromise (BEC) is one of the fastest growing and most financially damaging internet-enabled crimes.

In 2022, the total adjusted losses from BEC accounted for over $2.7 billion, as reported by the Internet Crime Complaint Center (IC3).

While BEC attacks can result in devastating financial losses for businesses, the long-term consequences, such as reputational damage and legal repercussions, can be equally significant.

What is BEC?

BEC, an acronym that stands for **business email compromise**, is a cybercrime whereby scammers assume the digital identity of a trusted persona to trick employees or customers into taking a desired action, such as making a payment or purchase, sharing data, or divulging sensitive information.

Why is it so hard to prevent?

BEC attacks rely heavily on social engineering techniques, along with weak authentication credentials. As a result, these attacks are difficult to detect or prevent with traditional security tools or spam filtering.

*Source: Protecting against coronavirus themed phishing attacks. Microsoft Security blog. March 20, 2020.

What are some examples of BEC?

INVOICE SCAMS

Attackers compromise a supplier's or vendor's email account and send altered invoices or payment instructions to customers. The altered details direct payments to the attacker's account, resulting in payments being diverted away from the legitimate vendor.

EMPLOYEE PAYROLL MANIPULATION

Attackers pose as HR personnel and request changes to an employee's direct deposit information. As a result, the employee's salary is redirected to the attacker's account.

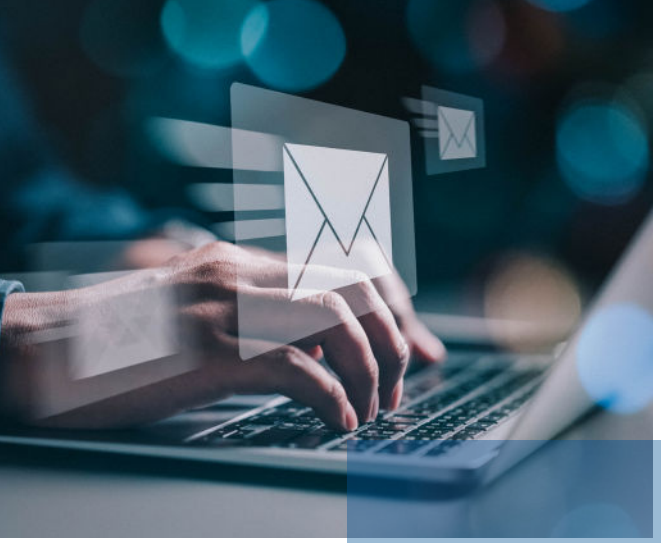
W-2 PHISHING

Attackers target HR departments during tax season, sending emails from the compromised company executive's account requesting W-2 forms or other sensitive employee information. This data is then used for identity theft or tax fraud.

ADMIN ACCOUNT TAKE OVER

Attackers compromise the IT administrator's account, who has full administrative access to the company's Microsoft 365 account. They then are able to read and manipulate the emails of any other employee in the company and create more administrative users in order to maintain access.

WESTON
TECHNOLOGY SOLUTIONS



How can I combat BEC attacks?

Since BEC attacks are generally human-centric, the methods of protection and prevention must also be human-centric. By partnering with us, you get access to a team of dedicated security experts who are working for you day and night to catch and contain BEC attacks.

Business email compromise is a serious threat. We can help you stay protected.

CONTACT US TODAY
to learn how we can protect your business against BEC attacks!

How can we help?

We possess advanced technology and specialized knowledge across various IT domains, including cybersecurity, enabling us to provide reliable solutions, proactive maintenance, and effective troubleshooting.

Additionally, you get access to a team of professionals at a fraction of the cost of building out your own security team, enabling you to concentrate on your core business.

We offer 24/7 monitoring of your IT systems, ensuring issues are identified and addressed promptly. This proactive approach minimizes downtime and disruptions and reduces the risk of breaches and data loss, which are crucial for businesses like yours.

How we protect against BEC

We have a powerful managed detection and response (MDR) solution included in our security services that secures your cloud identities and applications from BEC scams.

By detecting and responding to suspicious user activity, permission changes, and anomalous access behavior, and backed by a 24/7 SOC team, our solution empowers us to fight back against attackers on your behalf, with no gaps or lags in coverage during the peak seasons, off hours, or holidays.

WESTON
TECHNOLOGY SOLUTIONS