What Is Business Email Compromise?

Business email compromise (BEC) is a form of phishing that occurs when a cybercriminal impersonates a legitimate source to trick employees into wiring money, sharing sensitive information or engaging in other compromising activities. Typically, the cybercriminals behind a BEC attack will send a legitimate-looking email requesting payment for a business purpose. In such instances, cybercriminals may pretend to be senior-level employees, suppliers, vendors, business partners or other organizations.

Unlike more traditional phishing attacks that target large groups of individuals, BEC attacks are crafted to appeal to specific individuals—making them harder to detect and potentially more damaging. BEC is a threat that all businesses, regardless of size or industry, should take seriously.

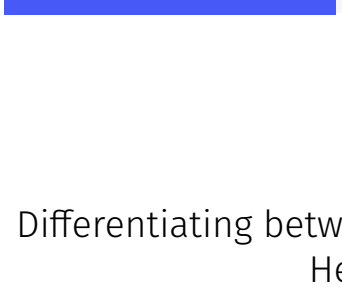
Common BEC Attacks

False invoice schemes—Cybercriminals pretend to be business suppliers and request fund transfers to complete an invoice.

CEO fraud—Criminals pose as high-level executives to request wire transfers.

Account compromise—Cybercriminals hack into an executive or employee account to request invoice payments directly from vendors.

Attorney impersonation—Hackers impersonate a corporate lawyer or law firm to request an immediate transfer of funds.



Data theft—Criminals pose as HR professionals or employees in other functional roles to obtain personally identifiable information or tax statements from other employees or executives.

Signs of a BEC Attack

Differentiating between legitimate business requests and BEC attacks can be difficult. Here are some signs that an email is a BEC attack.

Generic terms or lack of personalization

Variations to email addresses or company websites

Unfamiliar names or images

A sense of urgency or threatening language

Requests to send personal or financial information

Protecting Against BEC

BEC attacks can result in severe financial and reputational harm. Consider implementing the following cybersecurity practices to help reduce the risk for your organization.

Educate employees. Teach your employees to be wary of emails making requests, never click suspicious links and report any suspected BEC attack to IT.

Implement effective payment protocols. Ensure employees in charge of financial operations analyze invoices for validity and discuss them in person whenever possible.

Restrict access to sensitive data. Only provide access to sensitive data to trusted and experienced employees who require such information to conduct their work tasks.

Utilize security features. Ensure all organizational devices possess adequate security, such as antivirus and malware prevention programs, email spam filters, data encryption capabilities and a firewall.

Have a plan. Ensure your organization has an effective cyber incident response plan that specifically addresses response protocols and mitigation measures for BEC attacks.

For more cybersecurity and insurance guidance, contact us today.

VENBROOK INSURANCE SERVICES