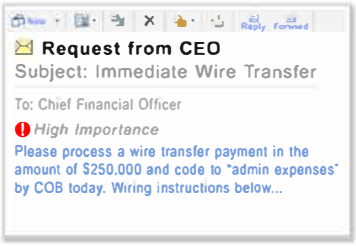
How to Recognize and Stop Invoice and Payment Scams

Invoicing and payment scam fraud can take a variety of forms.
Below are two common invoice fraud schemes and how you can prevent them.

These two scams are examples of a Business Email Compromise (BEC) -
when a corporate end-user account is taken over and used for malicious activities originating from a legitimate trusted email address.

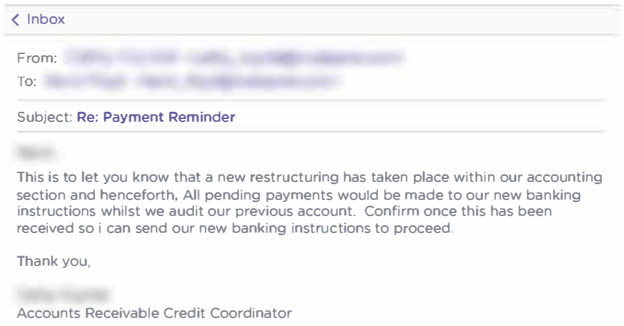
CEO Fraud/Impersonation

You receive a text or email from an executive with a request for an urgent financial transaction, but the message is a scam - the account has been taken over by an attacker. The authority of the sender, the urgency of the request, and the compromised email address create a very convincing hoax.



Vendor Impersonation

You receive an email from a trusted vendor, but the sender has enacted a BEC. They may tell you they've recently changed addresses or bank routing information, and attached an invoice, in an effort to collect money from you fraudulently.



Some Basic Things to Look for in Invoicing / Email Scams

As a precaution, avoid clicking links in emails that:

- Are not addressed to you by name, have poor English or omit personal details that a legitimate sender would include
- Are from businesses you are not expecting to hear from
- Ask you to download any files, especially with an .exe file extension
- Take you to a website that does not have the legitimate URL of the company the email is purporting to be sent from

Precautions and Best Practices

- Verify sender really sent email.
- Pick up the phone and call to verify.
- Check the phone number. Do not call the number in the email.
- Do not proceed with any wire instructions until proper verification is obtained.
- Do not be intimidated by proposed sender's title or status in the company.

Need Help Securing Your Business?

Contact Anjolen Inc:

Michelle Tuttle: mtuttle@anjolen.com