

Spotting Business Email Compromise

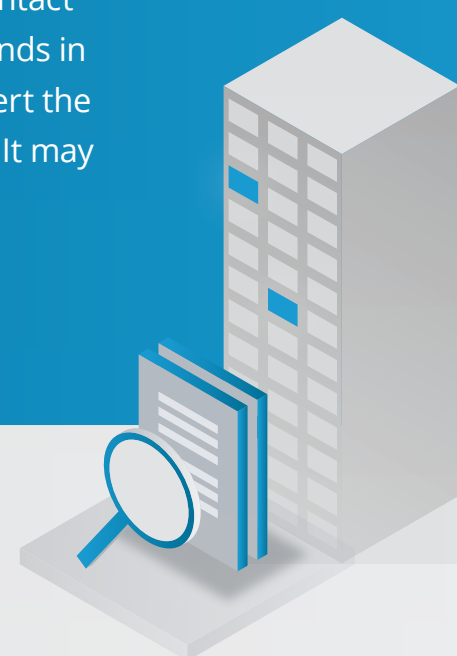
BEC attacks use sophisticated techniques that can trick all but the most attentive email users. Attackers typically impersonate a legitimate contact asking for a transfer of funds. But when victims send the money, it lands in a bank account controlled by the bad guys. The hackers quickly convert the money to crypto currency or shift it into other untraceable channels. It may be days before you even know you sent the money to an imposter.

Here are the key stages of business email compromise:

STAGE ONE

ID Target

Highly organized hackers use LinkedIn, company websites and other resources to identify executives, accounting employees and others who could be high-value targets. Social media lets them craft highly personal attacks using names of acquaintances, actual travel plans, etc.



STAGE TWO

Grooming Target

With their target selected, hackers begin using spearphishing emails, phone calls and other approaches to get targets to unwittingly give up their login credentials.

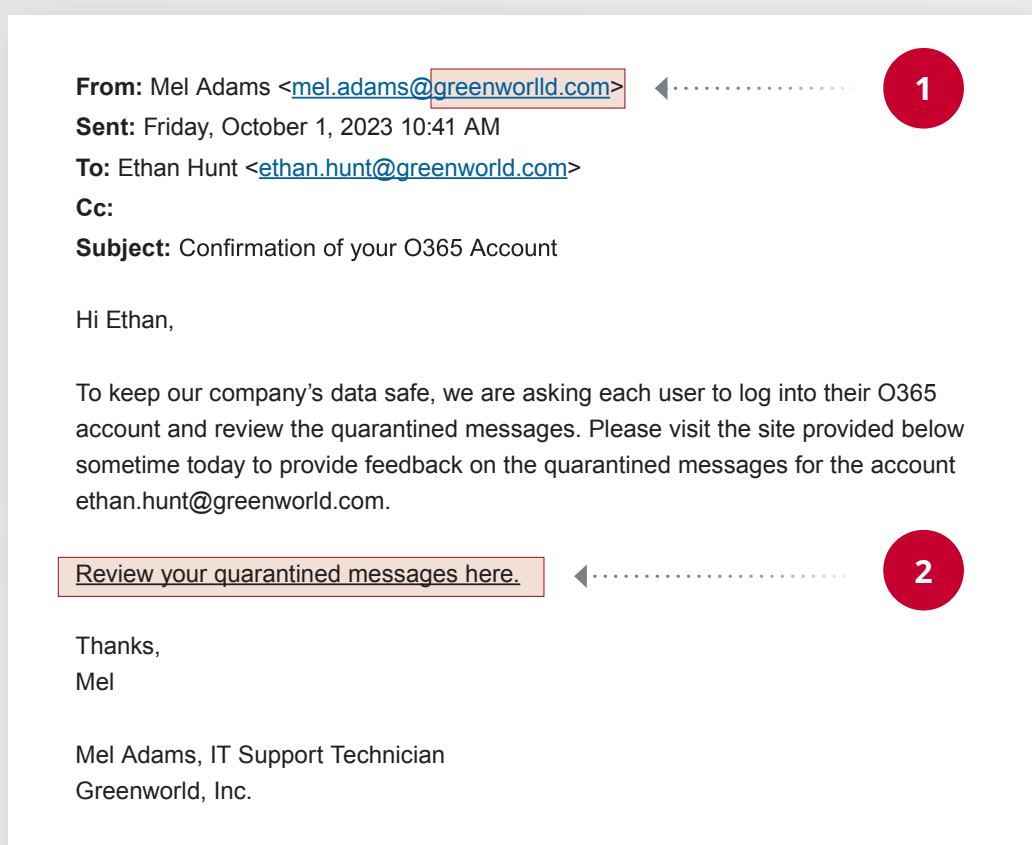


STAGE THREE

Transfer of Information

Hackers spring the trap by inserting themselves into an email thread and asking for a transfer of funds while posing as a legitimate contact.

↓ Message used to steal user credentials:



Red Flags of Business Email Compromise:

1. Spoofed address

Look carefully at the actual domain name, not just the sender's display name. This spoofed domain has an extra character in the company name.

2. Malicious link

This link actually leads to a credential harvesting site. Hover your mouse pointer over the link before clicking it to confirm that it's going to the expected address.

3. Real data used to fool you

Because hackers may be monitoring your email, they may jump into a legitimate thread. In this case, the first message in the sequence came from a real vendor talking about a real invoice. The hackers have inserted themselves and took over the discussion, cutting the real vendor out of the thread.

4. Timing

This is a fake email from the scammer, who sent the request late in the week, hoping to catch an employee rushing to complete tasks before leaving.

5. Suspicious attachments

If you're not expecting an attachment, don't open it. Call the sender to confirm it's a legitimate file.

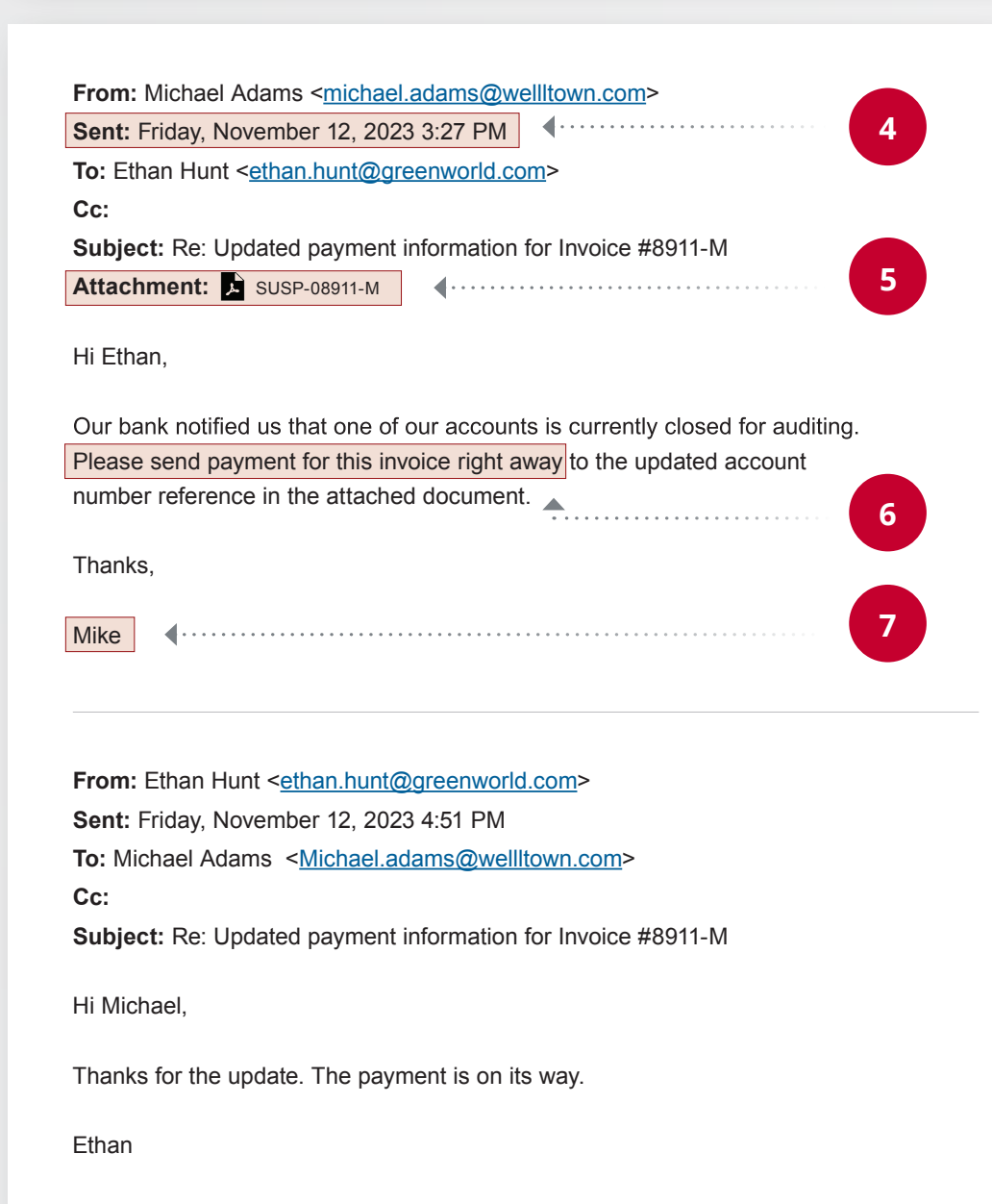
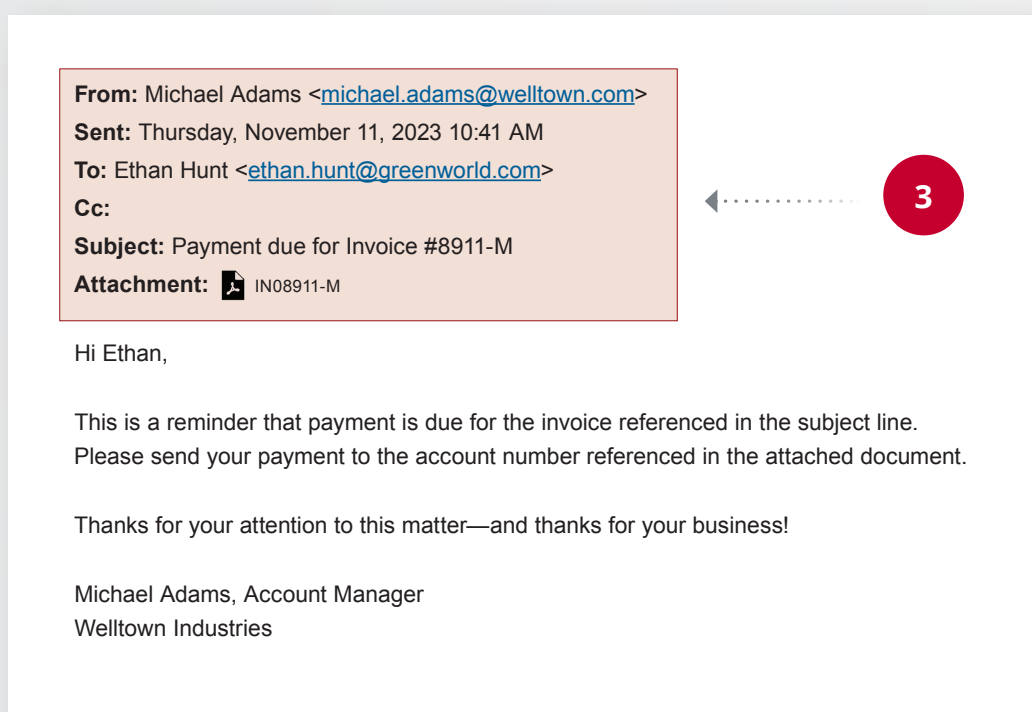
6. Sudden change in normal procedure and/or urgency

Be extremely wary of changes in deadlines, bank accounts, etc. Call your contact to confirm what's happening.

7. Unusual name usage

Hackers posing as legitimate contacts often fumble the details of names, so pay attention to any discrepancies, such as someone who normally goes by "Michael" signing a message as "Mike."

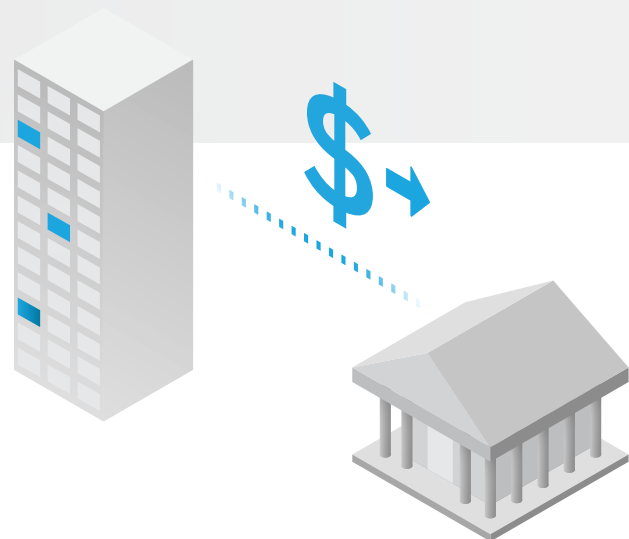
↓ Hacker takes over email thread



STAGE FOUR

Wire Transfer

Victims fall for the fraud by sending funds to a bank account that's actually operated by the criminals.



Train your teams to understand how to spot business email compromise and prevent potential attacks.