What's Your Game Plan?

Responding to Business Email Compromise

DEER BROOK

Business email compromise (BEC), also known as email account compromise (EAC), is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional.

In a BEC scam, criminals send an email that appears to come from a known source making a legitimate request, such as:

- A vendor your company regularly deals with sending an invoice with an updated mailing address.
- A contractor you work with sends new bank routing information for payments.
- A company CEO asked her assistant to purchase dozens of gift cards to send out as employee rewards. She's asking for the serial numbers so she can email them out right away.
- A home buyer receiving a message from his title company with instructions on how to wire his down payment.
- A banking customer is trying to add a signer to their account or change their email or street address in their profile.

Criminals will research your company and who you are conducting business with, and often impersonate them to trick you into trusting and unwittingly helping them.

How to Respond to Business Email Compromises

Every situation will be somewhat different. Use this as a reference with your technology resource to ensure all points are covered.

Identify

Identify what was affected, and where the damage is.

If you suspect wire fraud is involved, immediately contact your bank to initiate SWIFT recall messages. Perform recall processes, notify other banks involved, and request cooperation from your team and law enforcement as needed. Report the incident to the FBI through the IC3 website immediately. The report will go directly to a Fusion Center and be assigned to an agent. It is important to act quickly.

Double-check all wire and ACH information, including receiving bank, routing numbers, etc. to ensure that they are as expected. Consider a period of call-back verification with your bank for any transaction in doubt or any transaction that meets a certain limit to reduce risks of ongoing fraud potential.

Pay particular attention to any email requests to change payment types, payment terms, or locations that originated during the incident, especially from impacted accounts.

Review all outbound emails sent to understand who may need to be contacted or what may have been asked of them by the attacker.

Note all communications regarding the issue. Preserve any emails that may be related. Note how you discovered the issue or were notified. Note if any passwords were changed by the attacker.

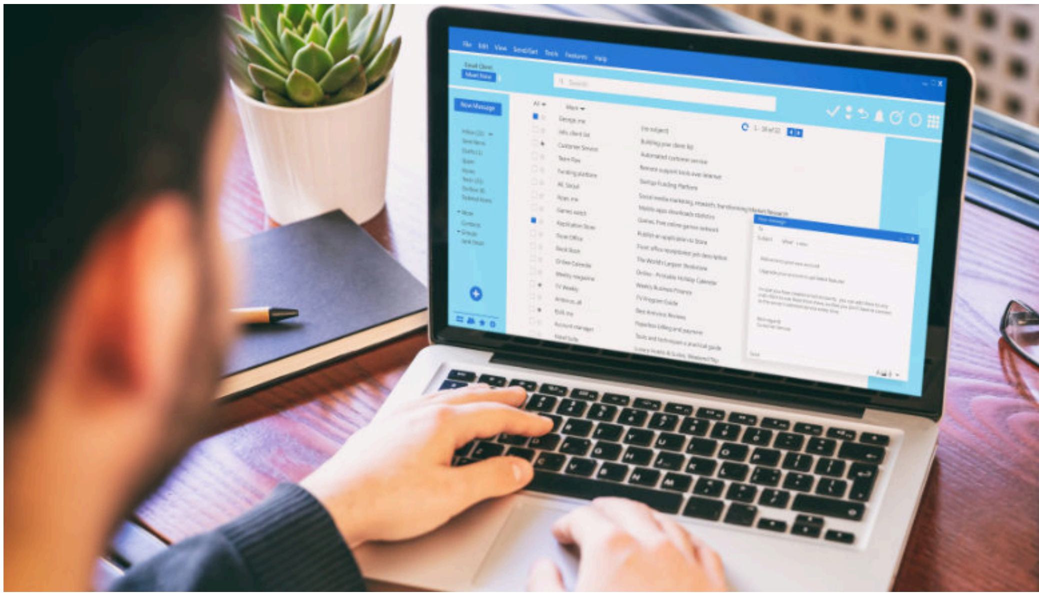
Ask the affected email user if they used the same username and password anywhere else. This is not the time to judge or reprimand them if they did. You need to know so you can take action to reduce your risk of greater compromise scope.

Contain

Contain what has been affected so that you can protect everything else from it.

Remove the user's computer from the network. Turn off Wi-Fi if it's connected to a wireless network. Leave it turned on, if possible, for your Information Technology resource to review.

Notify your Information Technology resource of the situation and provide this article to them. They may have additional tasks as well. Use this article as a guide.



Notify anyone who may receive a fictitious email from the compromised account.

Eradicate

Eradicate threats and close off any means used to compromise your email or systems:

- Change the affected user's email account password.
- Change all passwords for other online services that used the compromised email account as a verification email contact. Bad actors look for these to exploit them.
- Change passwords anywhere that the same combination of username and password was used.

If the email user has any financial responsibilities or access to finance systems or is authorized to conduct financial transactions, notify your bank, change online banking passwords, and change any finance system user account passwords.

If the affected user has administrator access rights to systems: change their administrator password and check activity event logs for any unauthorized activity conducted by their account.

Check their computer for malware with an antivirus solution. Verify that the antivirus is automatically updated daily and runs a full system scan at least weekly.

Verify that the computer's operating system is updated, and verify that all computer software, including web browsers, is updated

If available, review email log data for any information that can help identify the attacker and determine the scope of their access or activity, including remote IP, details of what was accessed, outgoing mail activity, etc.

Restore

Restore data and business functions, such as any lost data like deleted emails, email contacts, or attachments.

Once you're positive that your network is free of ongoing issues, contact any parties who need to know or to resume normal business operations.

Notify local law enforcement and obtain a police report. You may need this if you claim damages later.

Learn

Learn about what happened so you can prevent it from happening again.

Provide any emails sent by the bad actor from the compromised account to whomever is investigating. Emails need to be forwarded as attachments and not simply forwarded emails.

Train employees in safe computer use and how to notify the appropriate people if they experience or witness anything out of the ordinary.

Protect

Protect everything better, because now the bad guys know you're watching.

- Consider adding multi-factor authentication to email, network and finance system logons to prevent unauthorized third-party exploits.
- Review existing email protection measures. Recommended protections include spam filtering, email antivirus, Sender Policy Framework (SPF) referential checks, URL and attachment checks, and spoof protection.
- Add a banner in emails that declares if an email is from an external sender to help identify company account email spoofing.
- List all places where you would need to check in a hurry such as bank accounts and supply chain and payment bank routing information. A list helps so that there isn't a scramble during an incident.
- Test the effectiveness of your safe email handling training by periodically conducting email phishing tests.
- Hire or contract with a knowledgeable technology resource who understands information security.

Verify that you capture at least 30 days' worth of email and network (Active Directory for Windows) event logs so that data can be examined for forensic use. Review log settings for webmail systems and ensure that they will capture the appropriate information needed during an incident, including remote IP, details of what was accessed, and outgoing mail activity.

Final Thoughts

The most effective way to respond to a business email compromise follows this six-pronged approach: identify, contain, eradicate, restore, learn, and protect.