Business Email Fraud Scams

What They Are and How to Shut Them Down

Introduction

How could attackers trick you, an intelligent professional, into handing over company funds?

They impersonate someone you know and trust.

In business email compromise/email account compromise (BEC/EAC), also known as "business email fraud," a cyberattacker spoofs the email of someone within a specific company or someone associated with that company (a vendor, supplier or contractor). The attacker then assumes the identity related to that email account. He uses that identity to email a targeted victim, asking that person to make a bogus wire transfer or pay a fake bill.

Executive Summary

Attack Vector: Business email compromise

Targeted Organization: Cofense

What You Will Learn: How Cofense identified and shut down two business email fraud scams

Takeaways: 10 tips on how to protect your company against BEC/EAC attacks

The perceived authenticity of the emails has made the scams incredibly successful, and the number of scams has skyrocketed. According to the FBI's latest BEC/EAC alert, businesses worldwide experienced a 2,370% increase in actual and attempted dollar losses from BEC/EAC scams between January 2015 and December 2016.[1] Those losses – representing more than USD 5.3 billion – affected over 22,000 companies (large and small) in all 50 states and in 131 countries.[2]

2,370%

USD 5.3 Billion

in actual and attempted losses from BEC/EAC[4]

131 Countries

have recently been impacted by BEC/EAC scams[5]

Learn From Cofense's BEC Scam Experiences

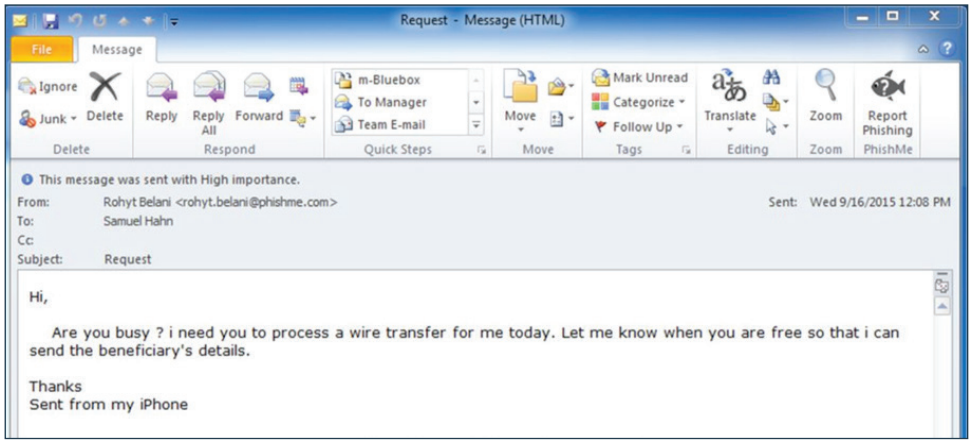
Since Cofense has been on the receiving end of numerous business email fraud threats and it's our business to defend against them, we have unique insight. In this report, we share play-by-play details on how the scams that targeted us began, how we reacted to them and what we did to turn the tables on the phishers. We also offer tips on how you can protect your company against BEC/EAC attacks.

We hope our experience and suggestions will help you address any business email fraud threats your company may face and save you from financial loss.

Case Study 1: How to Recognize, Respond to and Catch a BEC/EAC Scammer

Target: Cofense Executive

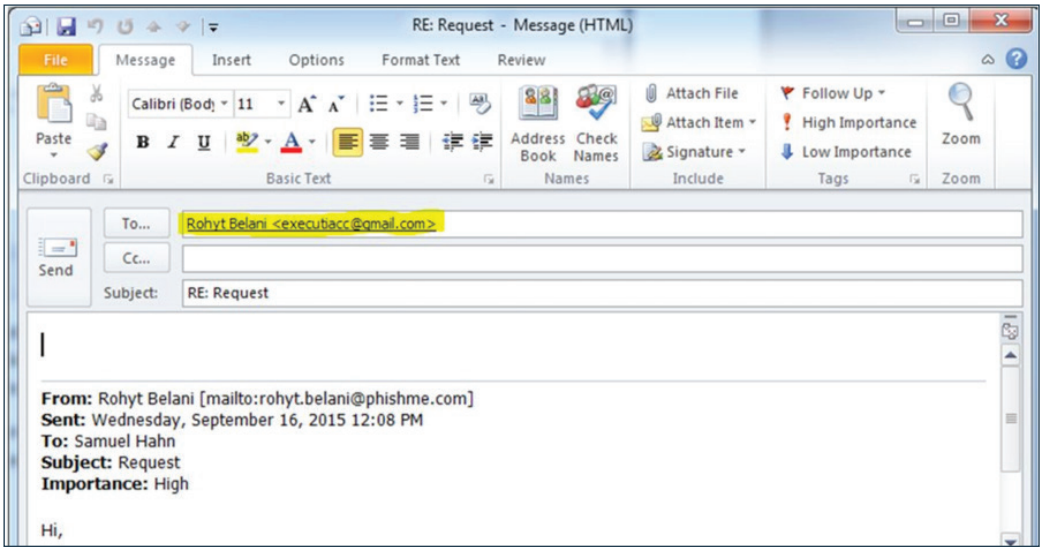
When BEC/EAC scammers first targeted Cofense on Sept. 16, 2015, they impersonated Cofense CEO Rohyt Belani in an email sent to Cofense Vice President of Finance Sam Hahn.



The attacker used the correct names and email addresses for Rohyt and Sam. (It's obvious he researched our company.) But, as you can see in the email, there are a few formatting mistakes (an extra space before "?") and punctuation errors ("i"). That's no surprise since errors in punctuation, spelling, grammar and formatting are common in phishing emails.

Two other details also grabbed Sam's attention, adding to his suspicions that this was a scam. The first was the greeting. Rohyt – even as personable as he is – doesn't usually start emails with "Hi." The second clue appeared below the signature line where the device used to send the message was listed. Sam knew the declaration "Sent from my iPhone" was a lie because Rohyt doesn't own an iPhone. He uses an Android smartphone.

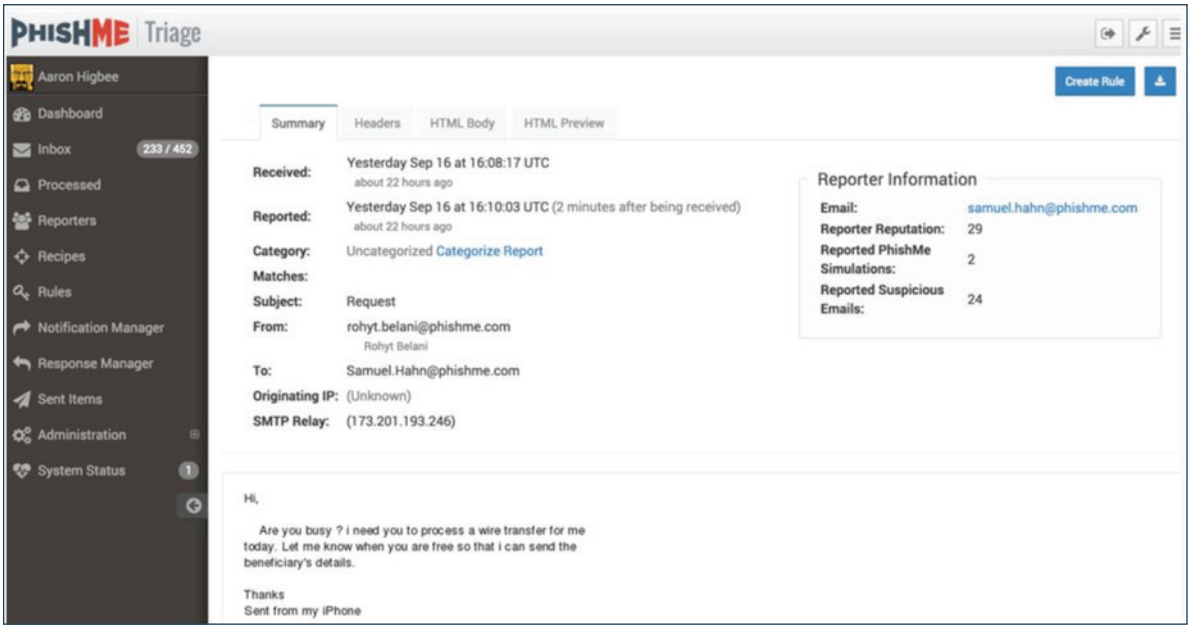
If Sam hadn't made those two observations, there was still a litmus test for confirming this message as a phishing email. And that was whether Rohyt's real email address (rohyt.belani@Cofense.com) would change when we replied to the email. It did.



The new address in the “To:” line was “executiacc@gmail.com” – not Rohyt’s real email address.

Knowing that a cybercriminal was trying to trick Sam, he did not reply immediately. Instead, he reported the threat by clicking a button in his email program. The button is part of a Cofense tool called Cofense Reporter™, which allows people to report phishing attacks in progress. Pushing the Cofense Reporter button immediately sends a notification to Cofense Triage™, a Cofense platform that collects and organizes reported threats so they can be investigated by a company’s IT incident response team.

Here is what Sam’s report looked like in Cofense Triage:



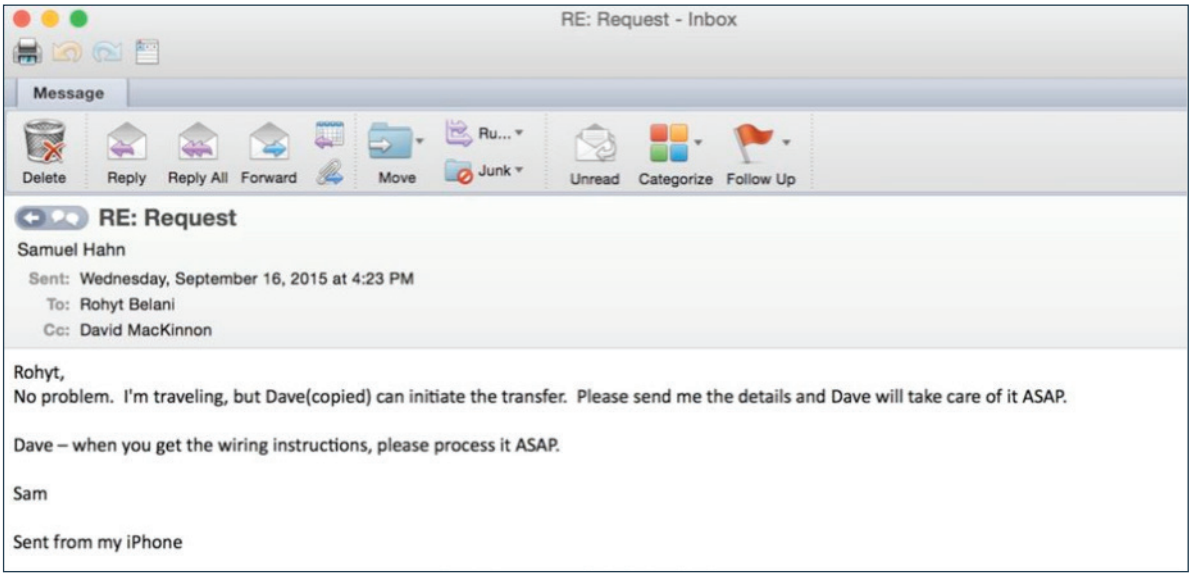
In the “Headers Tab” in Triage, we could see how the attacker spoofed the “From:” line (rohyt.belani@Cofense.com), yet he was still able to capture a reply by inserting a different address in this “Reply-To:” header:

```
Reply-To: Rohyt Belani <executiacc@gmail.com>
```

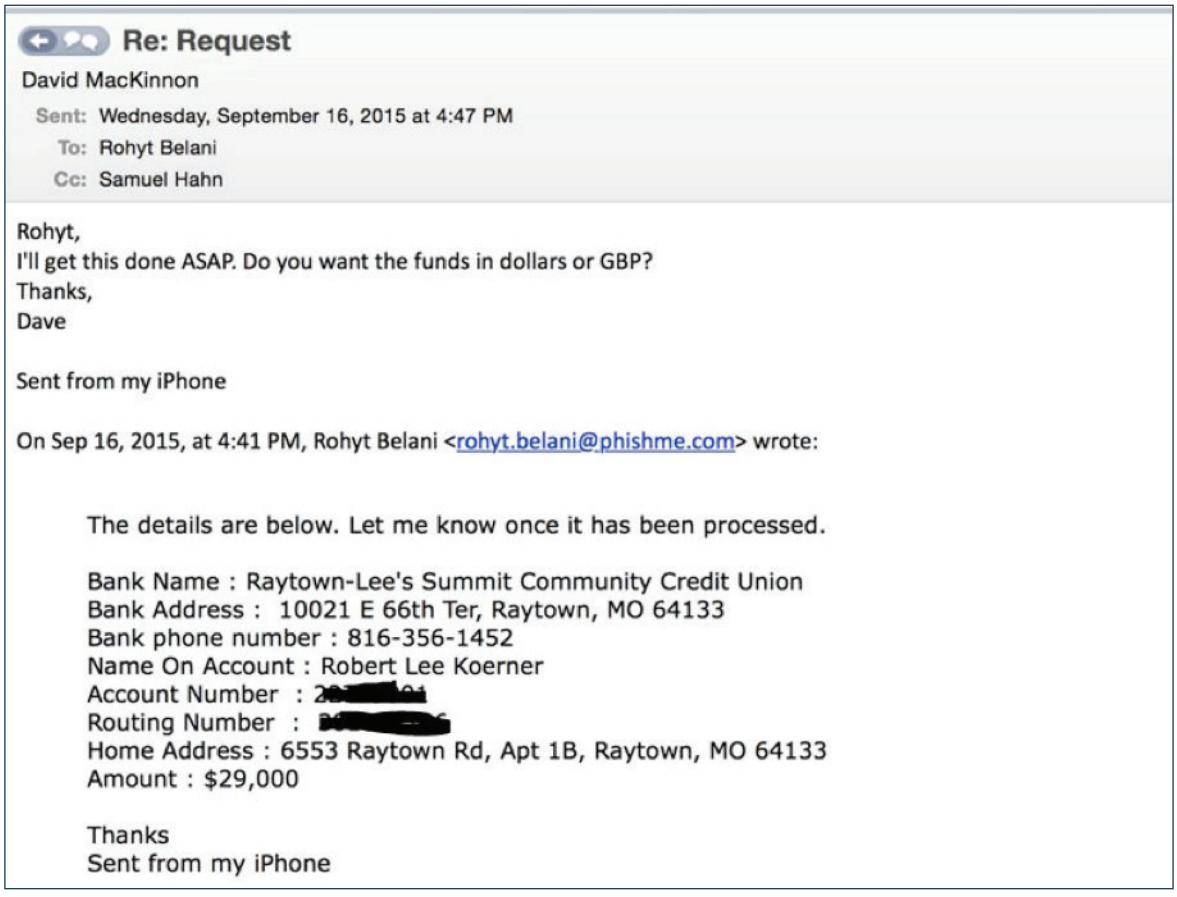
In considering how we would respond, we knew we had two goals:

1. To capture the receiving banking details so we could notify law enforcement and to determine if we were dealing with a human or an automated script

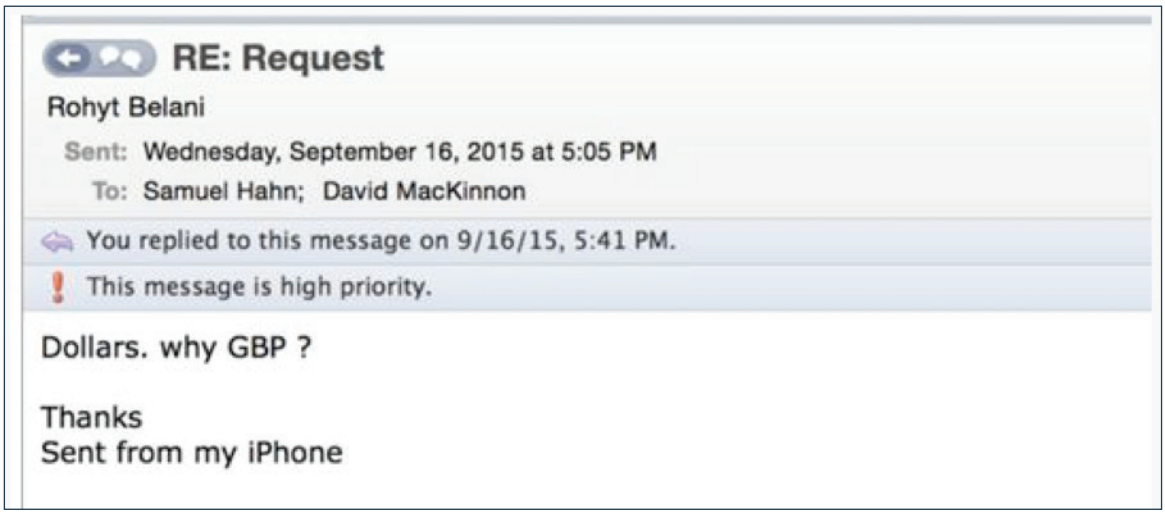
2. To accomplish this, Sam sent an email back to the attacker (“Rohyt”) and copied Dave (aka our Director of Incident Response), asking him to process the wire.



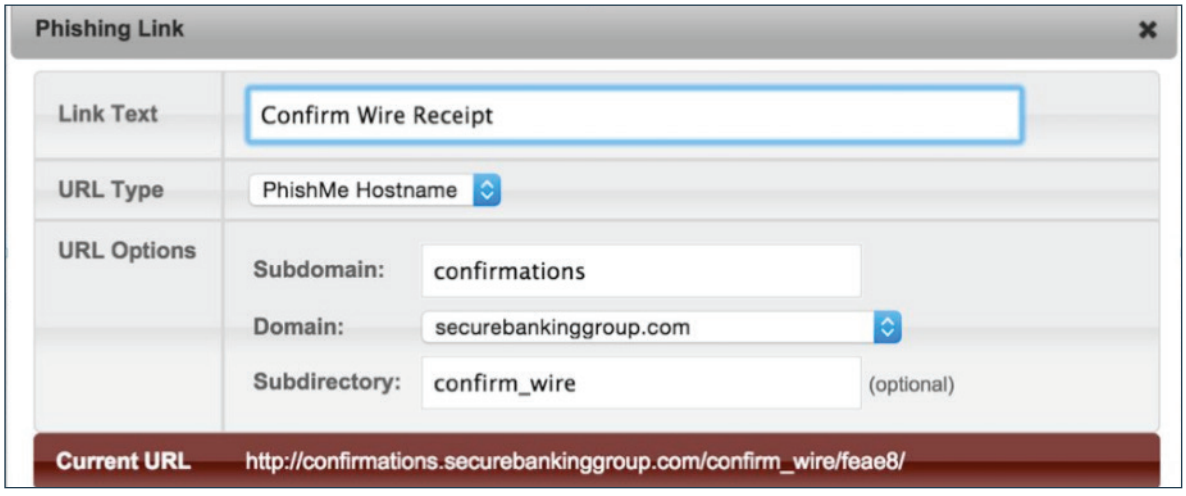
You can see below that goal No. 1 was achieved. We got a response back with some banking details, so we moved on with our second goal (to determine if we were dealing with a human or bot) by asking for clarification on the currency type.



This response below confirmed that a human was on the other end of our scam:



At this point we could have left well enough alone, but we own a tool that gives us the ability to track down an attacker's physical location. And we wanted to use it. Our Cofense Simulator platform allows us to send phishing emails to our clients' employees as practice – so they learn to identify malicious messages and NOT fall for them. The tool also allows us to extract the IP address of anyone who responds. So, we built an official-looking phish in Cofense Simulator and sent it to the attackers. This is what it looked like:



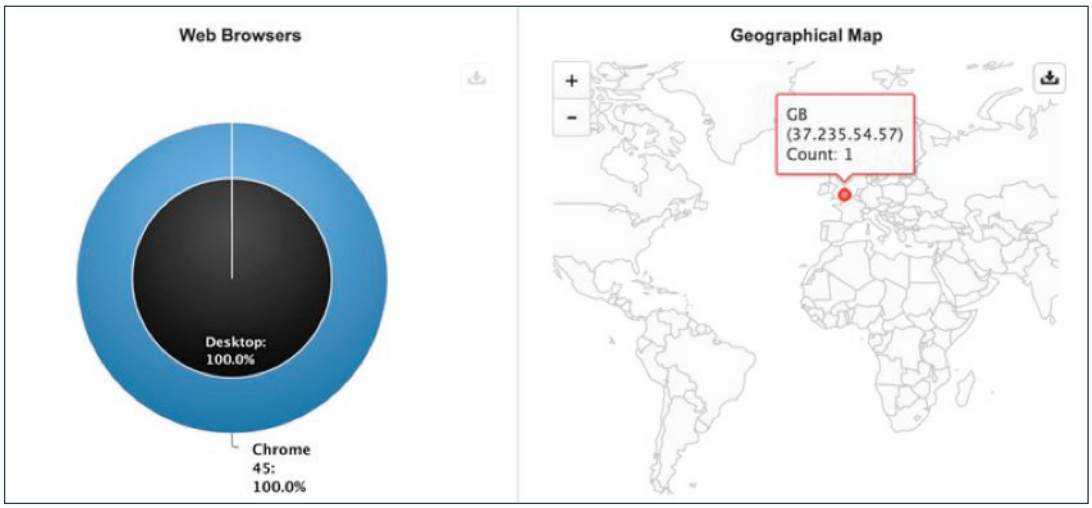
We then crafted a phishing email and sent it to the attacker ("Rohyt") to confirm the wire. We were not surprised when the attacker took our bait and clicked our phishing link, which allowed us to extract his host and IP address in the U.K. We immediately forwarded the information to law enforcement.

From: Finance <accountspayable@securebankinggroup.com>
Subject: Wire confirmation

Please take a moment to review wire information for Raytown-Lee's Summit Community Credit Union. Transaction details are available below:

Confirm Wire Receipt.

Accounting Department



We may never know why this fraudster thought phishing our company, an authority in cybersecurity, was going to be successful. But we shut down the attack and reported it.

Case Study 2: How to Recognize, Respond to and Catch a BEC/EAC Scammer

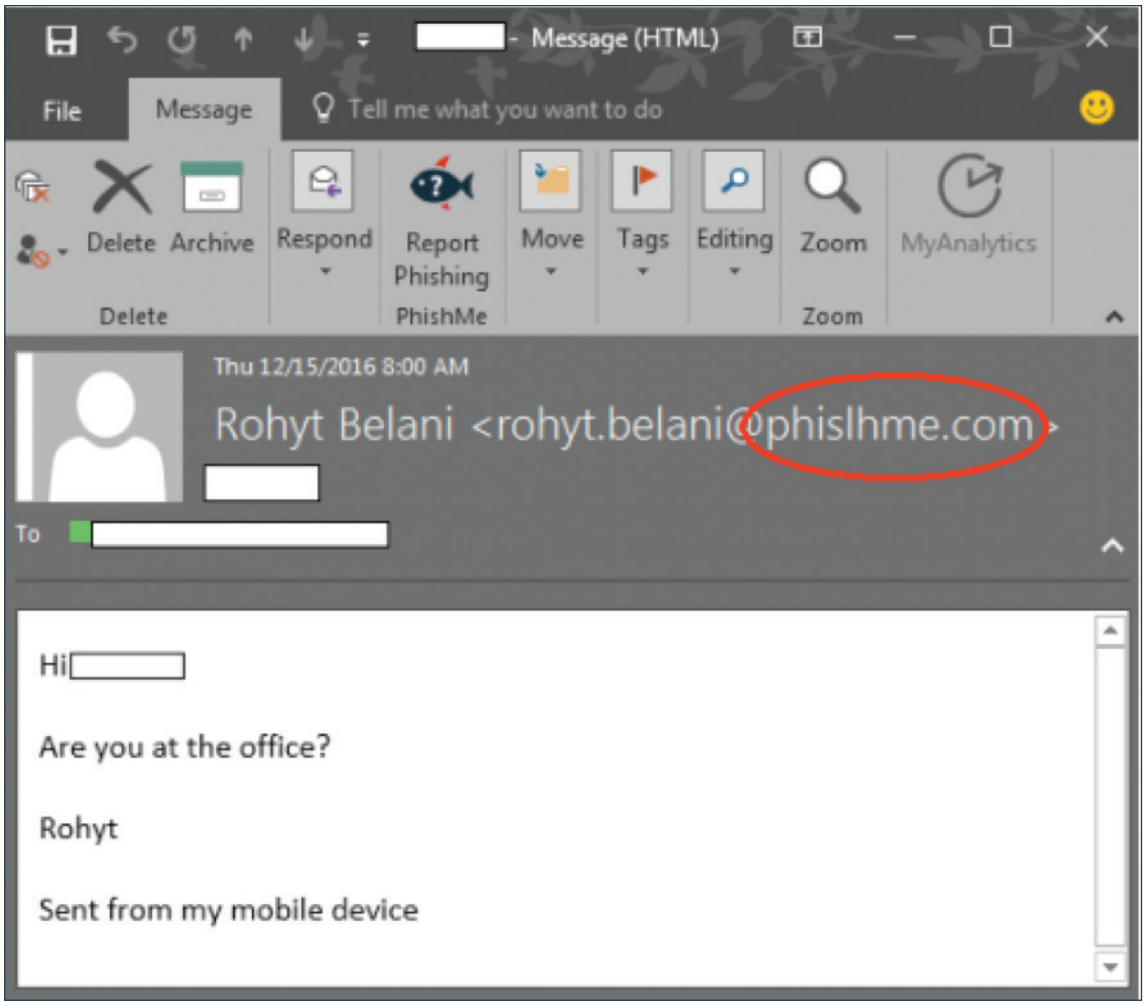
Target: Cofense Accountant

Since the September 2015 attack that targeted our CFO Sam Hahn, BEC/EAC scammers have repeatedly attempted to outwit Sam into making fraudulent wire transfers. When those attempts didn't work, the cybercriminals changed their tactic: Instead of targeting Sam, they targeted a Cofense accountant who reports to Sam.

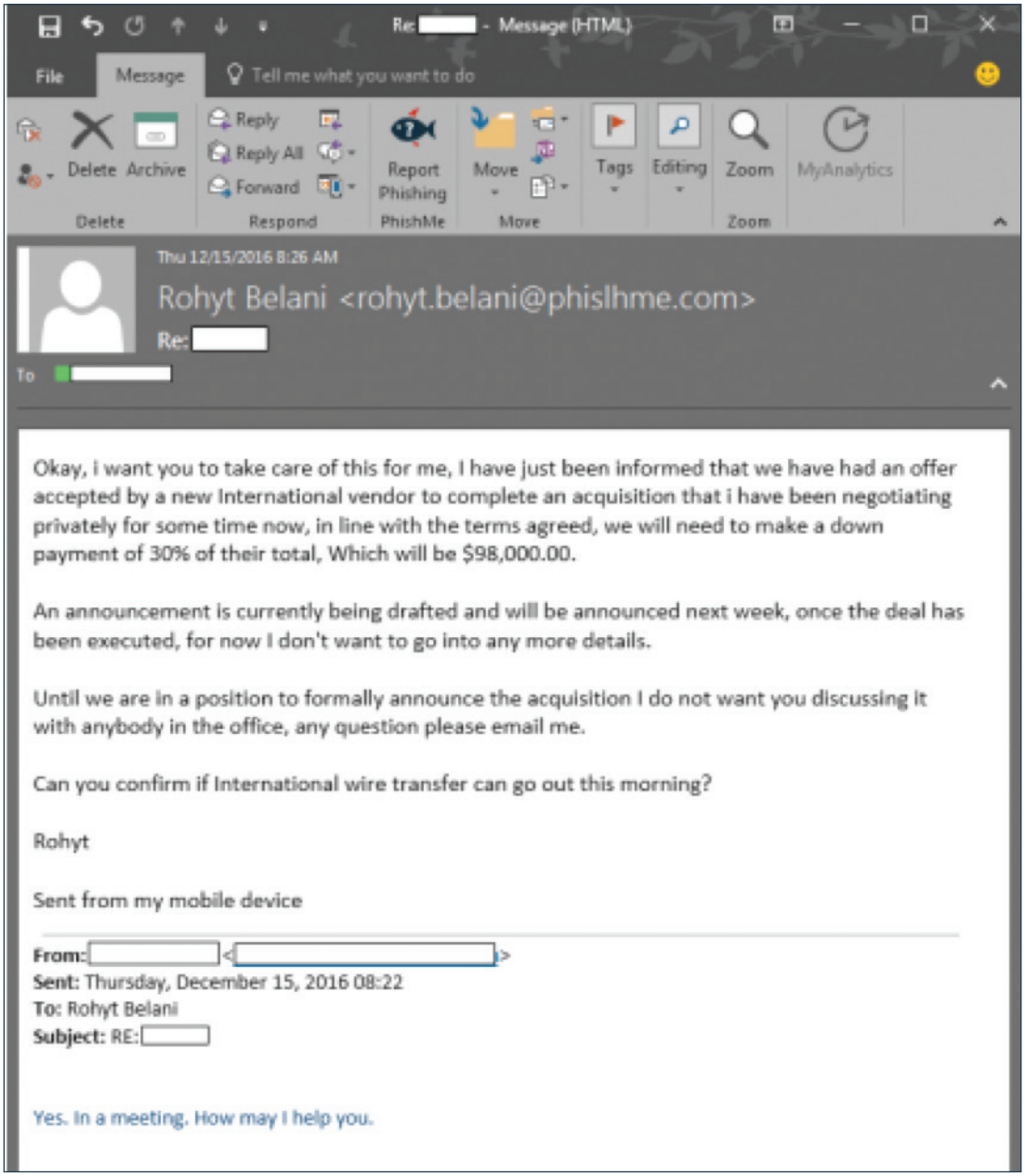
In the most recent attempt on Dec. 15, 2016, the phisher apparently used social media and/or search engine results to identify the name and email address of the accountant.

Our accountant, who is trained in using Cofense Reporter, used the tool to flag the message as "suspicious."

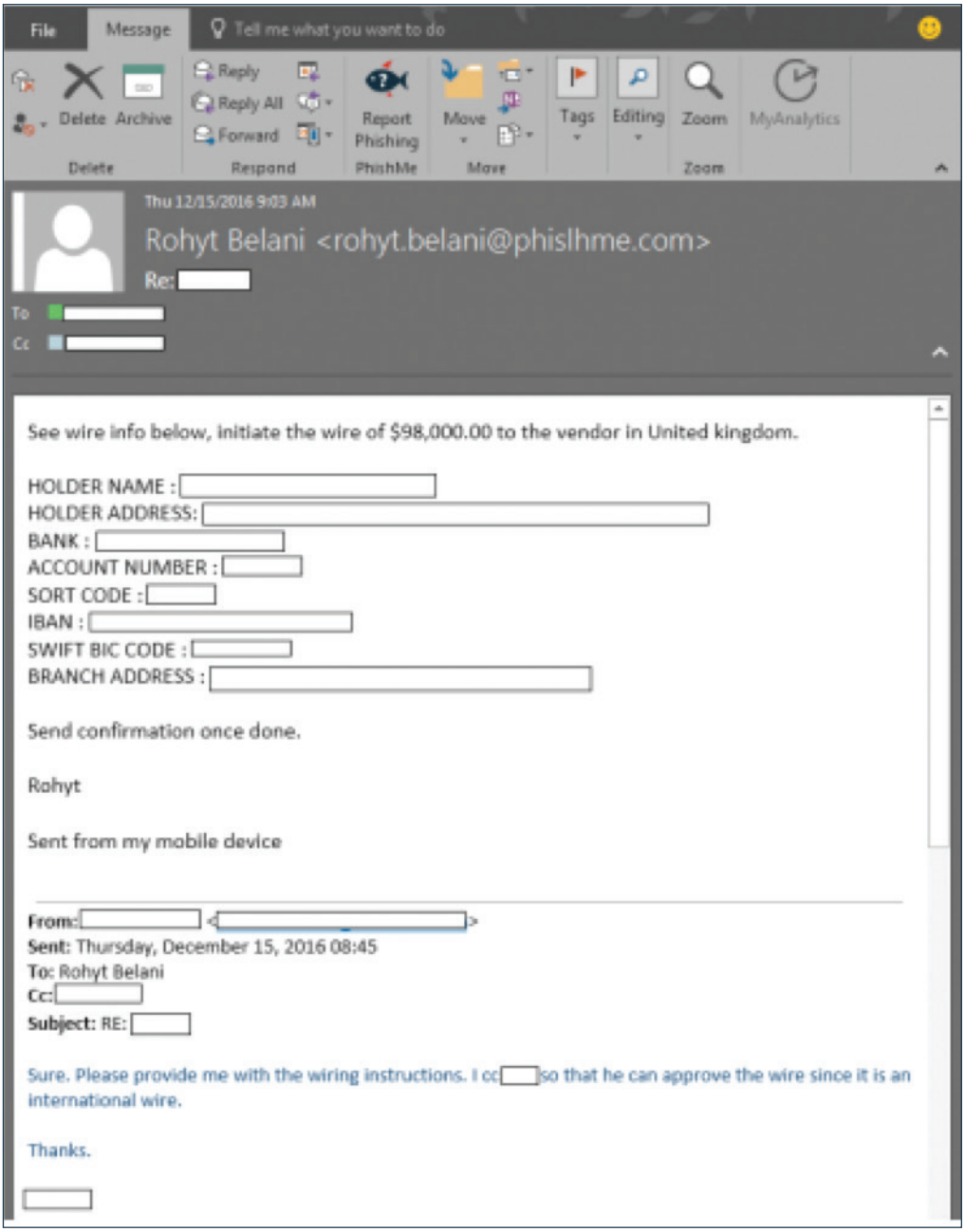
The subject line of the message looked real in that it had the accountant's first name and the salutation included her first name. But the request was suspicious in that the supposed sender was, again, our CEO, Rohyt Belani, and his email address was off by one letter. Instead of the correct email address in the "from" section (rohyt.belani@Cofense.com), the address included one addition letter ("l"): rohyt.belani@phislhme.com.



We played along with the ruse by then instructing our accountant to reply to the phisher with an offer to help, as seen in the figure on the next page. He responded right away with his plea for money to cover a secret international acquisition.

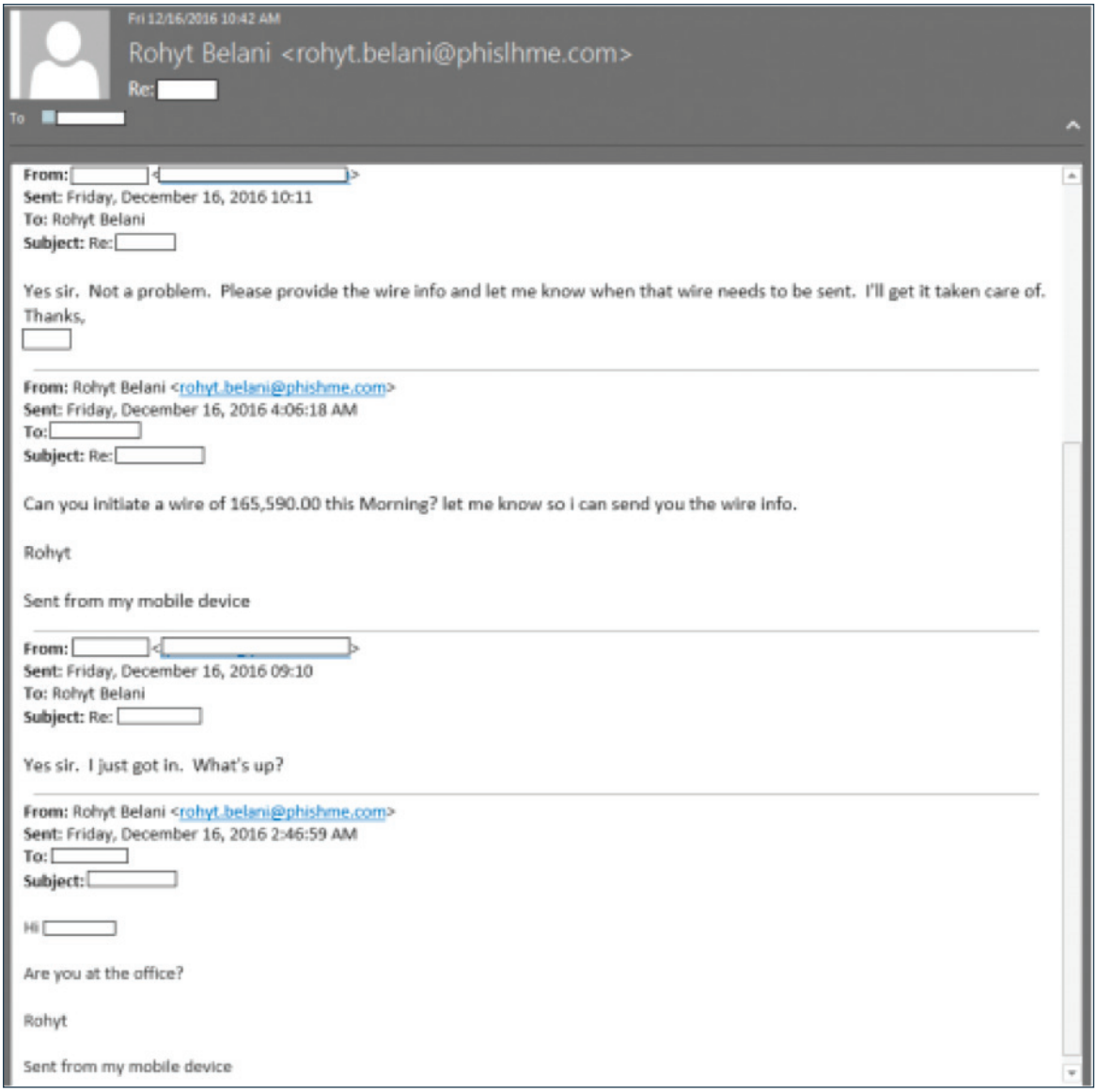


In her response to the message above, our astute accountant indicated that she would need an "associate" to sign off on the wire transfer "since it is an international wire." Her associate was a member of our incident response team, who later emailed the phisher a wire "confirmation link." The figure on the next page shows the third message from the phisher, where he sent wire instructions to the accountant.



Once the scam account was revealed, it was reported to the bank, and our incident response team member sent a “confirmation link” that, when clicked by the phisher, revealed the phisher’s physical location. What the phisher saw was the link redirected to the login page for the bank hosting the mule account.

The phisher must have been convinced that the wire transfer had been made because the next morning, 24 hours after the initial request, he came back for more money.



The final part of that email thread included instructions for a $165,590 wire, details of an account at a second bank and a request for a confirmation.

Beyond reporting this to the U.S. government's Internet Crime Complaint Center at www.ic3.gov, our researchers wanted to dig deeper and document this phisher's other activity.

It turns out that the lookalike domain name "phislhme.com" was registered at 1&1 Internet SE on Dec. 15, 2016, the same day as the first message to Cofense, using the email address garyrabine@rabinagroup.com. When we initially looked into whether that same email address had been used to register other domain names, we found 69 other domain names. They had all registered within the previous week and all seemed to be misspellings of domain names in use by real companies.

We took the list of domain names and guessed at which real company each domain was meant to imitate. We then notified the administrative contacts of record for those legitimate domain names. Though there were a handful of bounced messages, four companies replied with appreciation; and, so far, one has responded that their company had also received a BEC/EAC phishing email.

We checked back again later to see how many domain names had been registered with 1&1 by this threat actor and saw that there was a total of 156 domains. We notified 1&1 and requested that all the names be deactivated.

10 Tips: Protecting your company against BEC/EAC attacks

As you can see, business email fraud scammers are crafty.

There are, however, several steps you can take to protect your company against BEC/EAC attacks:

1. Establish a DMARC record on your company domain so that messages spoofing your real domain do not get delivered.
2. Enable two-factor authentication on your email accounts to prevent an attacker from hacking into your accounts and using them to send fraudulent messages. If your email provider doesn't offer this, change providers.
3. Minimize the number of people authorized to process and approve wire transfers within your organization.
4. Make a list available to employees with the names of those authorized to approve and process wire transfers.
5. Verify (with at least two people) any requests for new or different payment processes.
6. Create a threshold with your company bank for the maximum amount your company can withdraw through wire transfers so that banks can hold requests that go above the threshold for additional verification.
7. Be aware that hackers who impersonate executives often send business email fraud scam emails when the real executives are traveling on business.
8. Require dual authentication and approval for all wire requests:
   - Have the person requesting the wire transfer call you from a predetermined phone number to verify the request.
   - Call the person requesting the wire using a legitimate phone number (not from an email) and ask for a predetermined code to verify the person's identity.
   - Send the person requesting the wire a one-time code through a previously verified phone number to confirm the wire transfer request.
9. Adopt a comprehensive antiphishing program that empowers all your employees to act as the last line of defense against business email fraud scams. At the least, it should include:
   - A phishing simulations program, a scheduled process of periodically sending fake BEC/EAC emails to employees so they can become conditioned to what phishing messages look like.
   - A reporting tool that gives employees practice reporting phishing threats to your company's IT incident response team.
10. Identify specific, real-world phishing scenarios that your organization receives on a regular basis and; if your company uses a phishing simulation program, add them into your phishing simulation rotation.

Conclusion

Identifying and shutting down these business email fraud scams came easy for us because cybersecurity is our business. We're trained in the intricacies and iterations of phishing threats, including BEC/EAC scams. We have access to the most up-to-date phishing intelligence, and we have the right tools to deal with the threats.

Unfortunately, most people don't have the knowledge, resources or experience to combat business email fraud scams, and cyberattackers are clever. They use social media to find information that will help them impersonate people others trust. For that reason, BEC/EAC scams have been wildly successful.

Our No. 1 recommendation for helping businesses fight threats like business email fraud scams is to implement a comprehensive antiphishing program that educates, arms and empowers all employees to take an active role in defending the company – because all employees are targets. The program should give them the information, conditioning and positive support and encouragement to identify, report and mitigate threats.

Cofense offers companies a human phishing defense solution that includes the Cofense Simulator and Cofense Reporter, a combination that conditions employees to spot fraudulent email messages and report them to a company's IT incident response team.

For more information, contact Cofense or sign up for a free demo.

[1] FBI, "Business Email Compromise Email Account Compromise: The 5 Billion Dollar Scam," May 4, 2017.

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Ibid.

COFENSE

For more information contact:

W: cofense.com/contact T: 703.652.0717

A: 1602 Village Market Blvd, SE #400 Leesburg, VA 20175