An Insider's Guide to Business Email Compromise Attack Tactics & Prevention Strategies

By LMG Security

Business email compromise attacks have rocketed their way to the top spot on the FBI's list of most financially damaging internet-enabled crime, surpassing even ransomware. Global losses stemming from business email compromise totaled $43 billion since 2016 (including actual and attempted fraud).

The criminals are fast—too fast. The Microsoft Digital Defense Report found that the median time for criminals to access your private data after you are phished is 1 hour and 12 minutes. However, in LMG's private testing lab, **only 6 minutes elapsed between a successful phishing attack and the criminals logging in to peruse the victim's data**!

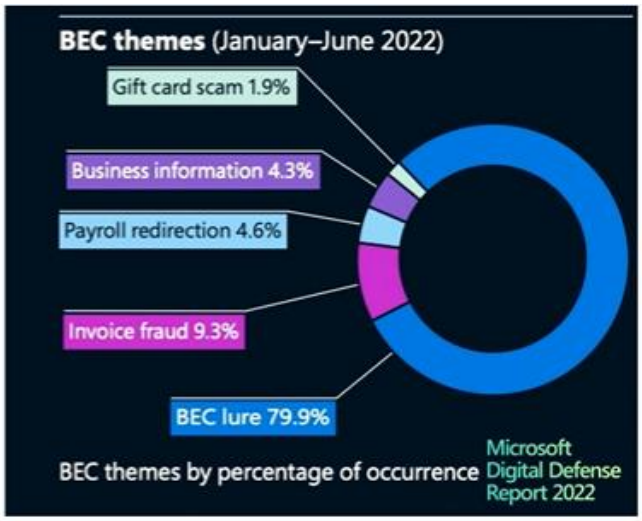
With over 24 billion stolen credentials circulating on the dark web, a business email compromise attack is an easy way for criminals to steal information, data, and money. Let's look at what business email compromise is, as well as the most common attack tactics and prevention strategies. Along the way, we'll also share a real-life step-by-step look at an actual business email compromise attack.

What is Business Email Compromise?

Business email compromise (BEC) is when cyber criminals break into your email for the purposes of financial gain. To monetize access to your email, the hackers may:

- Search for valuable data, such as Social Security Numbers, payment card information, tax details, W2s, or other personally identifiable information.
- Analyze your correspondence in order to identify opportunities for profit.
- Engage in **BEC scams**, in which the attackers trick you or a related person into sending them money.
- Reset your passwords for banking sites, social media, ecommerce, or other accounts to get access to more financial and personal information.
- Sell your passwords on the dark web.
- Send malicious emails to your contacts to acquire more victims and access.

Understanding the Most Popular BEC Scams



There are many different types of business email compromise scams. In 2022, the most common scams were:

1) **Invoice fraud.** Fake invoice scams are a lucrative tactic for criminals and the most expensive type of loss, on average. Attackers use their access to your email to find invoices and attempt to trick customers into sending payments to their accounts instead. Often attackers do this by creating spoofed invoices and emails that look just like the originals – but with different ACH or wire transfer details.
2) **Lures.** This is a very common tactic in which attackers send an email or text pretending to be someone you know – your boss, a colleague, a family member, or others – and ask you to send them money or information they can monetize.
3) **Business information theft.** Attackers often want information that they can leverage to commit a more complex attack. For example, attackers may pose as an executive and contact a finance clerk to request a customer list with contact information and amounts due. Then, the attackers contact each customer, requesting that they send payments to a new account number.
4) **Payroll redirection**. Attackers will email payroll or human resources contacts posing as a current employee and ask to change their direct deposit information to a new bank account.
5) **Gift card scams.** Attackers may send a text or email asking you to buy gift cards for your company or pay a bill or fine with gift cards.

Watch a Business Email Compromise Attack in Action

At LMG, we like to analyze hacker activities by watching them in action. Recently, we set up a business email compromise sting in our research lab. We created a fake company named HACKMe, Inc. with a victim employee named Sue Septebel Then, we "seeded" Sue's Microsoft 365 account with emails and files containing invoices, ACH requests, sensitive PII, and more.
Let's look at how the hack happens and what could have been done along the way to stop the attack. WARNING: Don't try this at home or work – we use a sandboxed lab computer to prevent infecting our environment.

1) Sue Septebel received a phishing email—and clicked on the link! (The link was taken from an active phishing site which our research team nabbed on openphish.com.) The email directed Sue to log in to a fake SharePoint Document Center to download the company's latest financial reports. The web site was a very realistic spoof with a URL that looked legitimate—the domain started off the same as the real site before devolving into a string of characters. The login page even had a valid SSL/TLS certificate! In this attack the criminals used a

passthrough with traffic going to Microsoft, but routing through the attacker's computer along the way. Sue could even sign in and use the site as usual—but the criminals were able to steal all of Sue's session cookies, tokens, and information necessary to hijack her account. Bottom line: You can't trust the lock icon anymore. Many cloud domain providers enable companies to click a check box and get a valid certificate for just a few dollars, and they don't actually check that you are who you say you are. So, take the extra step of checking each certificate carefully.

2) Within an hour, the criminals logged into Sue's fake account and searched her email and files for information. They started by searching for files with "invoice" in the name. Since this is a common tactic, we had an invoice ready for them from HACKMe's fake cleaning company, "Squeaky Clean Carpet Service."
3) The attackers then created a mail forwarding rule that automatically sent all emails with the terms "payment," "invoice," "wire transfer," or "personal" to their own external Gmail account. This is another common tactic used in business email compromise attacks to ensure that the criminals receive an ongoing stream of data from your hacked account. Since the emails were all still showing unread in Sue's account, most attacks would go unnoticed at this point. However, these attacks could be detected by checking the alerts logged in HACKMe's Microsoft compliance dashboard. Unfortunately, many organizations don't have their accounts configured to send an alert to responders when mail forwarding rules are created, so these signs of an attack are often missed.
4) At this point, the attackers downloaded the entire content of Sue's email account and any files they could access. Once this happens, it's usually game over for the victim and all emails in the account have been stolen. Typically, the next step in an incident investigation is to inventory all data that was in the victim's inbox in order to identify any sensitive data. Then, a qualified breach coach can determine whether notification to customers, employees, or other parties is necessary.
5) But it's still not over! The attackers continued to send Sue additional phishing emails to expand their access to her company's platforms and information. They searched Sue's files for recent invoices from HACKMe's vendors. They also downloaded the fake passport files from Sue's SharePoint account, as well as everything else they could find (note: with the right logging and configurations as part of your Microsoft account, you could get alerts for many of these activities).
6) Finally, the hackers created a rule to archive anything from HACKMe's vendor "Squeaky Clean," which had sent Sue an invoice. This is typically the final step that hackers take right before initiating an invoice scam. The attackers can now create a new monthly invoice or wire transfer request that looks exactly like the invoice they found in Sue's files with the additional note about a new account for payment. They then send it to Sue hoping she will switch the account numbers and give them a big payday!

How to Protect Against a Business Email Compromise Attack

We hope that the HACKMe BEC sting operation illustrated how easily these attacks can happen. Here is a checklist of strategies your organizations can use to prevent a business email compromise attack.

- Use **MFA and ensure it is configured properly.** Check out our MFA tip sheet or contact LMG with questions.
- **Review your email and cloud account configurations.** Misconfigurations enable security gaps and can result in your organization not receiving the alerts that can signal a breach! Pentests or cloud security assessments with a Microsoft 365 configuration review are a great way to catch these issues and reduce your risk.
- **Regularly review notifications.** Investigate immediately when you see a new forwarding or redirect rule is established.
- **Train your team.**
    - Prevent phishing with employee cybersecurity awareness training.
    - Put processes in place to verify all financial requests through a second, different form of communication. For example, if the request came in via email, call the requestor at a known phone number before acting on the request.
- **Formalize your reporting and resolution procedures.** If you need help with process and policy creation, contact LMG's advisory services team and we can help.
- **If you think your email has been compromised, you need to respond quickly!**
    - Lock out the attackers by changing your password and enabling MFA if you don't already use it.
    - Kill all active sessions. This cuts off any currently connected accounts and makes them sign in again, and they can't if you just changed the password.
    - Preserve evidence so you know if or what data was breached and what you may or may not have to report.
        - Download logs immediately. This provides records of access to your accounts
        - Place a litigation hold on affected accounts—you can check this box in your administration dashboard, and it will expand your storage and ensure the hacker cannot permanently delete any of the files.
        - Activate your data breach response process.
        - Call your cyber insurer and report the incident.
        - If you experience any type of financial fraud, immediately report it to the Internet Crime Complain Center at www.ic3.gov. They have a recovery access team that has relationships with many financial institutions and can quickly freeze assets to increase the possibility of recovering any fraudulent payments.

We hope you find these tips helpful. We wish you a happy, healthy, new year that is free from business email compromise!

This blog is distributed with the permission of LMG Security.

ABOUT LMG SECURITY

LMG Security is a full-service cybersecurity firm, providing one stop shopping for a wide array of cybersecurity services. Whether you need virtual CISO or regulatory compliance consulting services, testing, solution integration, training or one of our many other services – our expert team has you covered. Our team of recognized cybersecurity experts have been covered on the *Today Show* and *NBC News*, as well as quoted in the *New York Times*, *Wall Street Journal*, and many other publications. In addition to online cybersecurity training, LMG Security provides world-class cybersecurity services to a diverse client base located around the United States and internationally.