Monthly Newsletter July 2024

THE BSS ADVISOR

IT that Cares since 1995 www.bssconsulting.com

bss Business System Solutions

Business Email Compromise: What it is and How to Prevent it

Photo by Pixabay/Gerd Altmann

Reprinted with permission from the National Cybersecurity Alliance, a non-profit resource for advocation and education of businesses, families, and individuals about cybersecurity and keeping all safe from Cybercrime. Find out more at https://staysafeonline.org.

While it has a bland name, Business Email Compromise (BEC) refers to a specific, nasty type of cyberattack that targets businesses of all sizes. This sophisticated hack targets email communication within organizations. When successful, BEC can lead to financial losses, reputational damage, and compromised sensitive information.

What is Business Email Compromise?

At a basic level, BEC is a type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential company info. The cybercriminal spoofs a person or organization the target knows, like a supplier, and asks for a fake invoice to be paid, sensitive company information, or other data they can profit from. Cybercriminals can even use BEC to spread malware within an organization's network by convincing employees to click a fake link or download a malicious attachment.

BEC attacks are increasing, especially as many organizations have employees working from home or in a hybrid work scenario in the

(Continued on Next Page)

Business System Solutions is your IT Service Partner who provides peace of mind through guidance, education, and responsive support. We are IT that Cares.

Serving:
North Central Indiana
(765) 742-3440

Middle Tennessee
(615) 819-0600

West Michigan
(616 776-0400

info@bssconsulting.com

"For the Lord is good and his love endures forever; his faithfulness continues through all generations."
Psalms 100:5 NIV

(Continued from page 1)

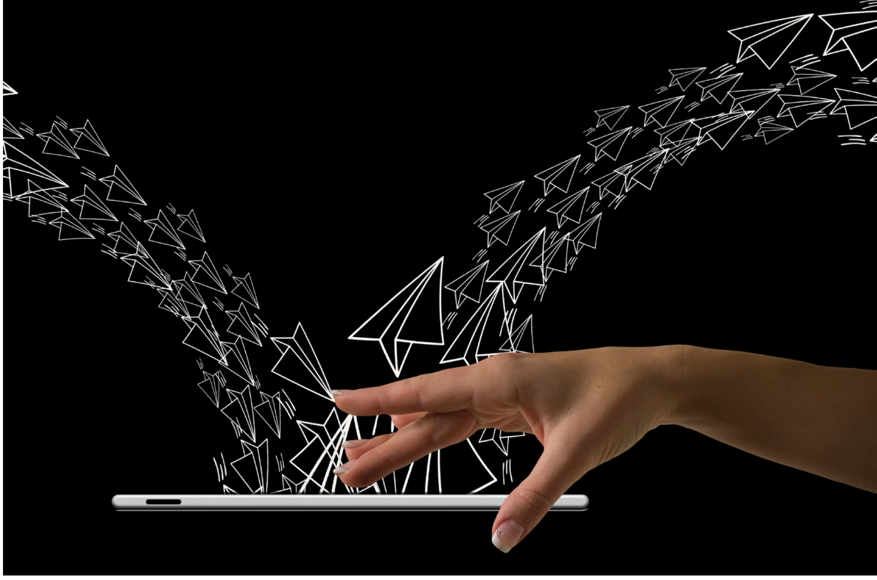

Photo by Pixabay/Gerd Altmann

wake of the COVID-19 pandemic. According to a recent report from software company Fortra, almost a quarter of emails that were delivered to corporate email inboxes in the first few months of 2023 were deemed "untrustworthy or malicious." While ransomware grabs many headlines, BEC is a huge cybersecurity issue for all companies.

Understanding the Tactics

BEC attacks come in various forms, but they are, essentially, a sophisticated, targeted evolution of phishing that focuses on organizations. In conducting a BEC attack, the hackers attempt to make their emails look as legitimate as possible and usually impersonate trusted entities like colleagues, suppliers, or executives. The attackers might even know about the person they are phishing, like their name and position. BEC emails might ask directly for money by asking for a fake bill to be paid, or they might ask for bank account information. On the other hand, they might request data, documents, or for the target to click on something that spreads malware.

If your employee or supplier's email account is compromised, the attackers can hijack actual email conversations and ask to reroute payments or update direct deposit info, for example. Disable email forwarding outside of the organization – your system administrators can do this.

How to protect yourself and your company from BEC scams

Train your employees

The first line of defense against BEC is a well-informed workforce. Conduct regular cybersecurity awareness training sessions to educate employees about the risks associated with phishing emails, the importance of verifying sender information, and the reality of BEC attacks. Our 2023 Oh Behave survey found that 94% of respondents made some sort of behavior change after cybersecurity training, with over a third saying they started using multi-factor authentication and around 50% saying that they developed a better eye for phishing.

Adopt email authentication protocols

Implement email authentication protocols such as DMARC (Domain-based Message Authentication, Reporting, and Conformance) to verify the authenticity of incoming emails. DMARC helps prevent domain spoofing and ensures that emails originating from your domain are legitimate.

Verify the sender

Whenever an email asks for money or sensitive information, verifying the sender through another form of communication is always smart, especially if the request is unexpected or strange. Call the supposed sender using a known phone number (not one in the suspicious email) or by meeting face-to-face.

Enable MFA

Your organization should enforce MultiFactor Authentication (MFA) across all email accounts within your organization. MFA adds another layer of security beyond passwords and significantly boosts your security. When implemented across an organization, MFA reduces the risk of unauthorized access even if login credentials are compromised.

Software updates

Make sure your software is running the latest versions. Keep email servers, antivirus software, and other security tools up to date to protect against vulnerabilities. These regular updates ensure that

(Continued from page 2)

your defense mechanisms can handle the latest threats.

Incident response plan

Your company should develop, and regularly update, an incident response plan to outline what will happen in the event of a BEC attack. The plan should include procedures for isolating systems, alerting relevant authorities, and communicating about the attack.

Email encryption

Use email encryption software to keep the contents of the emails hard to crack. Encryption ensures that even if an attacker gains access to email communications, the information remains unreadable without the appropriate decryption key.

Implement financial controls

All organizations should strive to maintain rigorous financial controls, especially when it comes to authorizing wire transfers or sensitive transactions. Implement a two-step verification process for financial transactions to minimize the risk of unauthorized transfers and changes to account numbers or payment methods.

Audit and monitor

Conduct regular security audits to identify and address vulnerabilities in your email system. Continuously monitor your system to detect unusual or suspicious activities, which enables a swift response to suspected BEC incidents.

Don’t be compromised by BEC

BEC remains a threat to businesses and other organizations, but with proactive prevention strategies and robust mitigation, businesses can strengthen their defenses. Foster a culture of cybersecurity awareness and stay vigilant against evolving threats. All these actions help you prevent BEC, as well as many other security threats. □

Original article: https://staysafeonline.org/resources/business-email-compromise-what-it-is-and-how-to-prevent-it/

Multi-Factor Authentication for All

Earlier this year, Microsoft announced that Multi-Factor Authentication (MFA) would be required to access any Microsoft account. In an effort to provide the best protection against BEC and other threats, BSS is implementing MFA for all our clients using Active Directory and Microsoft 365.

Why is MFA becoming mandatory? The simple answer is that it can prevent an attack or compromise of your personal or business accounts by requiring a second way to confirm it’s really you logging in. If your account is only protected by a password, a threat actor can easily brute force their way into your accounts. From there, they will be able to steal or send emails, change bank routing information, or access other, more critical parts of your business or network to drop ransomware or exfiltrate data.

BSS offers two versions of MFA depending on the needs of your staff. Your Technical Account Manager will be working with you shortly to setup and train your employees on how to get started with MFA.

If you have questions or concerns, please reach out to your Account Manager or drop a line to support@bssconsulting.com. □

bss Business System Solutions

Return Address:
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544

The BSS ADVISOR

info@bssconsulting.com

North-Central Indiana Office
1211 Cumberland Avenue
West Lafayette, IN 47906
(765) 742-3440

Middle Tennessee Office
1026 West College Street
Murfreesboro, TN 37129
(615) 819-0600

West Michigan Office
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544
(616) 776-0400

6 Years in a Row!
2019-2024 Winner
Channel Futures
Leading Channel Partners Forward
MSP 501

Upcoming Events

Tennessee

7/30, 12-2 PM
MTC NETWORKING & BACK TO SCHOOL EVENT

Michigan

9/5, 11:30-1:30 PM
CLIENT APPRECIATION LUNCH

Indiana

9/18, 11:30-1:30 PM
CLIENT APPRECIATION LUNCH

Tennessee

9/26, 11:30-1:30 PM
CLIENT APPRECIATION LUNCH

Details for all events at
bssconsulting.com/news-events

BSS Ranked #202 on Channel Futures' Global MSP 501 List

We're thrilled to announce placement on Channel Futures' MSP 501. The MSP 501 is a coveted and prestigious list of the top IT Managed Service Providers from countries around the globe.

Out of more than 15,000 applicants, BSS has been ranked spot #202. Channel Futures uses a quantitative methodology and applicants must pass a rigorous review, including financial performance, long-term company health, committment to reoccuring revenue, and operational efficiency.

2024 marks the sixth year that BSS has achieved this milestone. For more details, visit bssconsulting.com/news-events.

Channel Futures™
Leading Channel Partners Forward