Business Email Compromise (BEC) & Healthcare

May 16, 2024

TLP:CLEAR, ID# *202405161300*

Agenda

- The Phishing Hierarchy
- Types of Business Email Compromise (BEC)
- How Business Email Compromise (BEC) Works
- Spotting A Business Email Compromise (BEC) Attack
- Prevention, Awareness, & Reporting

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

The Phishing Hierarchy

Understanding Business Email Compromise's Place in the Phishing Hierarchy

Let's Start at the Top: Phishing

- Phishing involves an attacker using spoofed emails and websites—usually purporting to be from a friend or well-known business—as lures to dupe individuals into voluntarily handing over sensitive accounts, or other login information, online.
- The use of "ph" in place of the "f" in the spelling of the term is because some of the earliest hackers were known as "phreaks".
  - Phreaking refers to the exploration, experimenting and study of telecommunication systems. As phreaks and hackers have always been closely linked, the "ph" spelling was used to link phishing scams with these underground communities.
- The first time the term "phishing" was used and recorded was in January 1996.
  - The mention occurred in a Usenet newsgroup called AOHell.
- Designed to take advantage of the fact that so many people do business over the internet, phishing is one of the most prevalent cybersecurity threats around, rivaling distributed denial-of-service (DDoS) attacks, data breaches, etc.

Source: iStock

The Next Level: 2024's Top Types of Phishing

- **Email Phishing:** The attacker sends an email that looks legitimate but is designed to trick the recipient into entering information in a reply, or on a website that the hacker can use to steal or sell their data.
- **Vishing (Voice Phishing):** This is when someone uses a phone call to try to steal information. The attacker may pretend to be a trusted friend, a relative, or a representative of some kind.
- **Clone Phishing:** Involves a hacker making an identical copy of a message the recipient already received; they may include an additional message like "Resending this!" with a malicious link in the email.
- **Pharming:** The victim gets malicious code installed on their computer, and this code then sends the victim to a fake website designed to gather their login credentials.
- **HTTPS Phishing:** This attack is carried out by sending the victim an email with a link to a fake website. The site may then be used to fool the victim into entering their private information.

The Next Level: 2024's Top Types of Phishing, cont.

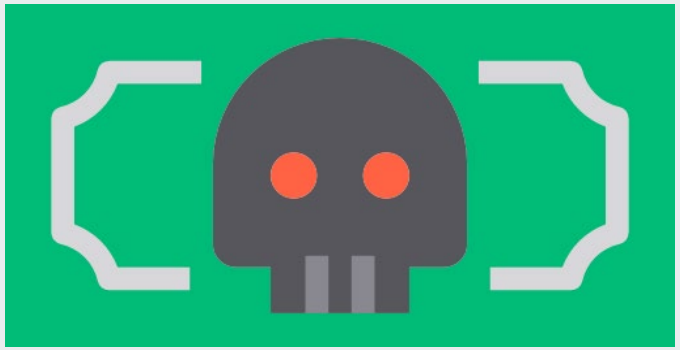
- **Pop-up Phishing:** Often uses a pop-up about a problem with your computer's security, or some other issue, to trick you into clicking; you are then directed to download a file, which ends up being malware, or to call what is supposed to be a support center.
- **Smishing:** Phishing through some form of a text message or SMS.
- **Evil Twin Phishing:** In this attack, the hacker sets up a false Wi-Fi network that looks real. If someone logs into it and enters sensitive details, the hacker captures their info.
- **Quishing:** A cybersecurity threat in which attackers use QR codes to redirect victims to malicious websites or prompts them to download harmful content.
  - HC3 Product: QR Code-Based Phishing (Quishing) as a Threat to the Health Sector
- **Spear Phishing:** Involves targeting a specific individual in an organization to try to steal their login credentials. The attacker often gathers information about the person before starting the attack, such as their name, position, and contact details.

Business Email Compromise (BEC)

- Business email compromise (BEC) is a spear phishing attack that utilizes social engineering.
  - HC3 Product: Social Engineering Attacks Targeting the HPH Sector
- It is one of the most damaging and expensive types of phishing attacks in existence, costing businesses billions of dollars each year.
- 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.

Business Email Compromise (BEC), cont.

- These attacks do not rely solely on technical vulnerabilities, but exploit the human tendency to trust authority, act impulsively, and respond emotionally to urgent requests.
- The following BEC statistics were reported to the FBI IC3, law enforcement, and derived from filings with financial institutions between October 2013 and December 2022:
  - Domestic and International Incidents: 277,918
  - Domestic and International Exposed Dollar Loss: $50,871,249,501
- The following BEC statistics were reported in victim complaints to the IC3 between October 2013 and December 2022:
  - Total U.S. Victims: 137,601
  - Total U.S. Exposed Dollar Loss: $17,328,435,141



Types of Business Email Compromise (BEC)

Five Types of Business Email Compromise (BEC) Scams

- Attorney Impersonation
- CEO Fraud
- Data Theft
- Account Compromise
- False Invoice

Note: *In the examples we will be sharing, you will notice that attackers utilize more than one of these scam methods in their attacks.*

Attorney Impersonation

- An attacker will pose as a lawyer or legal team member, and pressure or manipulate the employee into acting, such as sending data or requesting a wire transfer.
- Since the request is typically framed as urgent, confidential or both, it typically takes advantage of the fact that low-level employees within an organization are likely to comply with requests from a lawyer or legal representative, because they do not know how to validate the request and simply comply to avoid negative consequences.
- **Example:**
  - **Victim:** Facebook and Google
  - **What Happened:** Evaldas Rimasauskas and associates set up a fake company named “Quanta Computer” — the same name as a real hardware supplier. The group then presented Facebook and Google with convincing-looking invoices, which they duly paid to bank accounts controlled by Rimasauskas. Along with the fake invoices, the scammers prepared counterfeit lawyers’ letters and contracts to ensure their banks accepted the transfers. This resulted in around $121 million in collective losses.

CEO Fraud

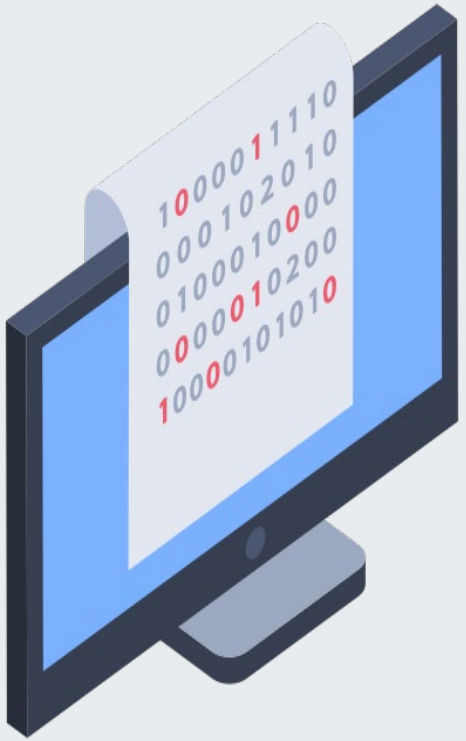
- Similar to an attorney impersonation attack, except the attacker poses as someone with executive authority, such as a CEO or other C-suite executive.
- In most instances, the attacker will target a member of the finance team claiming to need urgent support on a time-sensitive or confidential matter that may not be verifiable with anyone else. The "CEO" could say they are meeting with a vendor and discovered that the last payment did not go to their new account. In these events, the employee is goaded into transferring money into an account controlled by the attacker.
- Takes advantage of the power dynamic within the company and uses social engineering tactics like urgency, scarcity, and specificity.
- **Example I:**
  - **Victim:** Freight and logistics provider, Scoular Co.
  - **What Happened:** An employee received an email supposedly from their boss, the CEO. The email informed the employee that Scoular was set to acquire a Chinese company. The CEO instructed the employee to contact a lawyer at accounting firm KPMG who would help facilitate a transfer of funds and close the deal. The employee obeyed, and soon found themselves transferring $17.2 million to a Shanghai bank account. Scammers had used email impersonation to create accounts imitating both the CEO and the KPMG lawyer.

CEO Fraud, cont.

- **Example II:**
  - **Victim:** A children's hospital, for millions of dollars
  - **What Happened:** This particular hospital became a target for fraud after kicking off a project to build a new campus and publicly announced who the general contractor would be. The threat actor was quick to jump on this news and launched a BEC attack spoofing the construction company's email domain. This individual also impersonated the firm's CFO and sent a letter to the hospital using a fake construction group letterhead and requesting that payments be directed to another account.
- **Gift Card Scams:** Victims receive an email from attackers masquerading as an authority figure, asking victims to purchase gift cards for personal or business reasons.
  - This type of attack is particularly common during the holiday season and Black Friday.
- **Example:**
  - **Victim:** A synagogue
  - **What Happened:** In 2019, attackers impersonated rabbis and convinced synagogue congregants to purchase gift cards for a fundraiser, telling them to send pictures of the serial numbers on the back.

Data Theft

- Not only designed to steal money from a company, this type of attack targets HR and finance personnel and attempts to steal sensitive information about an organization's employees. This information can then be sold on the Dark Web or used in planning and executing future attacks.
- **Example:**
  - **Victim:** Snapchat
  - **What Happened:** Cybercriminals launched a BEC attack against social media firm Snapchat. Impersonating Snapchat's CEO, the attackers obtained payroll information about some current and former employees. The scam resulted in a breach of highly sensitive data, including employees' Social Security numbers, tax information, salaries, and healthcare plans. Snapchat offered each affected employee two years of free credit monitoring and up to $1 million in reimbursement.



Account Compromise

- An employee's email account is hacked and used as a vehicle for financial or data-related crimes.
- In many cases, the attacker will use the account to request payments on behalf of vendors. These funds are then transferred to accounts owned or controlled by the attackers.
- **Example:**
  - **Victim:** A children's charity
  - **What Happened:** The attacker gained access to an employee's email account, and from there sent fake invoices and other documents pretending that the money was needed to pay for a health center's solar panels in Pakistan. The charity had had a base there for decades, so the attack was well-researched and effective, and before the scam was exposed, the money ($1 million) had already been deposited in a Japanese bank account.

False Invoice

- Often seen when working with foreign suppliers, in this scam the attacker poses as a vendor and requests payment from an employee for a service.
- In most cases, the attacker will present themselves as an actual vendor and edit an official vendor invoice template. However, the attacker will alter the account details so that funds will be transferred into an account owned by the hacker.
- **Example I:**
  - **Victim:** A government health insurance program in several states, and two private insurers
  - **What Happened:** The victim entities were scammed into wiring payments in a series of schemes involving several fraudsters in multiple states. In most of these schemes, the cybercriminals created email accounts that looked almost identical to legitimate businesses and hospitals. Targets were tricked into updating bank account details for reimbursement payments. To hide their gains, several of the fraudsters used stolen identities to open bank accounts in the name of shell companies.

False Invoice, cont.

- **Example II:**
  - **Victim:** A church
  - **What Happened:** Hackers pretended to be the construction firm that had repaired the roof of a church, and emailed parish officials claiming that they had not been paid in two months. The parish swiftly wired $1.75 million into a fraudulent account, and the perpetrators swept it out before anyone knew what had happened. As a result, the parish resolved to start sending manual checks again instead of wire transfers to stop any future fraudsters in their tracks.
- **Example III:**
  - **Victim:** North Rhine-Westphalia (state in Germany)
  - **What Happened:** The threat actors in this case cloned the website of a real supplier of protective equipment from Spain. They compromised the supplier's email and used it to contact officials from the German health authority, who purchased what they assumed was equipment from a real company, wiring the money to the specified accounts. Once the actors received the money, they quickly moved it from Europe to Nigeria and escaped immediate consequences. Fortunately, the INTERPOL and German authorities intervened, and the money was eventually refunded to the health authority, but the state almost lost the equivalent of 14.7 million dollars.

How Business Email Compromise (BEC) Works

The Four Phases of a BEC Attack

A BEC attack can be broken down into four parts:

- **Phase One:** Research
  - During this phase, the criminal will collect publicly available information about the company they plan to impersonate and will be targeting from various online resources.
- **Phase Two:** Prepare
  - The actor will use the information they have gathered to attempt to gain access to the company's email system through various means.
- **Phase Three:** Execute
  - After gaining email access, the attacker will send targeted, high-pressure emails to trick employees into handing over protected information.
- **Phase Four:** Disseminate
  - If successful, the attacker takes the money and runs.

Phase One: Research

- Over days or even weeks, attackers perform deep reconnaissance, meticulously gathering information to determine what organization to attack, and then everything about that particular organization.
- They will:
  - mine the company website for contact information or to determine the typical email address format,
  - leverage an organization's social networks to research names and titles of various team members, as well as their roles and responsibilities,
  - read press releases and news,
  - and will try to find out confidential business information about the company on the dark web.
- During this phase of reconnaissance, they will also familiarize themselves with some of the following:
  - specific business processes,
  - workflows involved in different employees' day-to-day responsibilities,
  - who is responsible for making payments,
  - and details about payments made to vendors (schedules, banks, etc.).

Phase One: Research, cont.

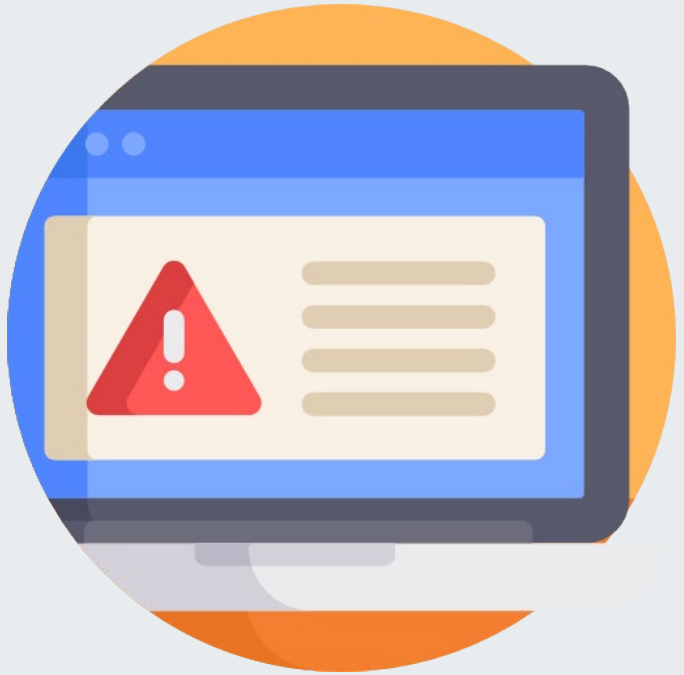
- As they did with the organization, threat actors research the people they will impersonate (typically focusing on someone at the executive level*, but really it can be whoever they believe is best suited to convince the company's staff to wire them money) learning:
  - their personal information on social media sites,
  - the employee's general Internet presence,
  - geographical location,
  - and other sensitive data.
  - *Note: Something that works against an organization is that individuals at the executive level are typically the faces of their organization—meaning it is really easy to track their digital footprint and launch a successful BEC attack.
- Once the hacker identifies their attack technique and assumed identity, they then go on to conduct research on who they are going to target. This could be anyone in the company, but often these people will be legal professionals, people who directly report to high-level executives, or employees entrusted with the organization's payment authorizations.

Phase Two: Prepare

- With the identity and target set, the attacker will then prepare other components of the attack, which include:
  - Domain spoofing
    - A domain appearing to be legitimate at first glance, but a closer look will reveal that a W is actually two Vs, or a lowercase L is actually a capital I.
  - Creating a fake company website
  - Social engineering
  - Setting up bank accounts
  - Create invoices or any other asset the attacker will need to substantiate their identity or the request
  - Compromising accounts
  - Using malware to infiltrate company networks and gain access to legitimate email threads about billing and invoices
- Attackers will use at least one, if not more of these components in the preparation phase.

Phase Three: Execute

- BEC scammers will use their digital identity to manipulate or pressure the target to take a desired action by using a single email or a series of emails with detailed specifications, personalization, and time sensitivity to make the malicious email seem more authentic.
- They will also leverage elements of influence, insistence, and legitimacy to convince the victim, ensuring the person acts on the request without discussing it with another employee or fully thinking through the scenario.



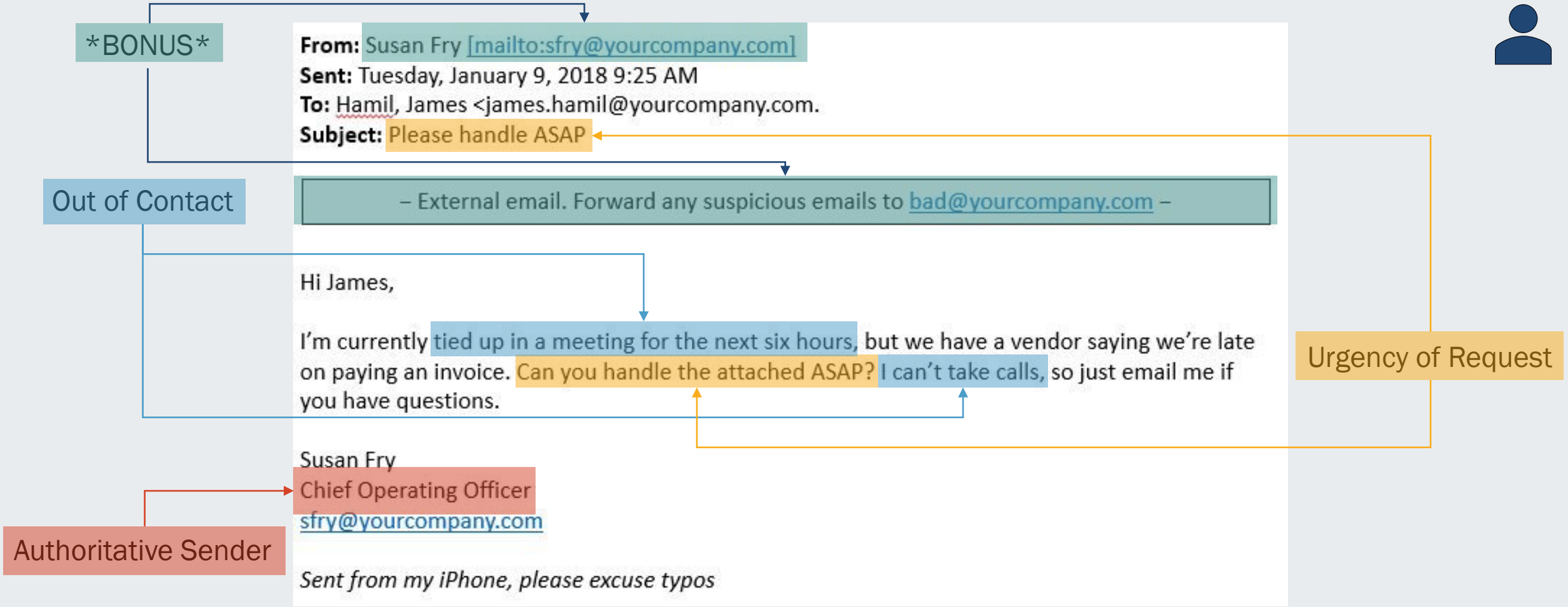
Phase Four: Dissemination

- If successful, the attack will end with the transfer of money, data, or other information to the hacker.
- Once the money has been wired, the threat actor quickly collects and spreads it across several accounts to reduce traceability and retrieval chances.
  - It is critical to respond rapidly to BEC attacks. Organizations that are slow to identify BEC attacks are unlikely to recover the money.

Spotting A Business Email Compromise (BEC) Attack

Know the Signs…

- **Authoritative Sender:** BEC attacks require the actor to impersonate someone authoritative.
- **Urgency of Request:** A request to transfer funds is sent with a pronounced sense of urgency. Actors launching a BEC attack strive to get the target to act quickly before they realize they are being scammed. To achieve this goal, the actor uses words like ‘quick,’ ‘urgent,’ ‘important,’ ‘soon,’ and ‘reminder.’ These words usually appear in the subject line but can also appear inside the email.
- **Different Domains:** Email communication originates from an unknown or spoofed domain.
- **Out of Contact:** Requestor is unreachable but insists on the urgency of the transfer. Threat actors try to prevent their target from reaching out to the impersonated person using another communication channel. The goal is to ensure the target does not realize that the email is fake. Threat actors do this by instructing the victim not to contact the sender or attempt to confirm the request with others.
- **Language and Grammar:** Syntax is different or erroneous. Emails are not in the standard context normally encountered or for alternate business purposes while requesting a transfer of funds.
- **Secrecy:** Email sender requests that information about transfer be kept secret.
- **Specific Instructions:** Threat actors launching BEC attacks usually provide clear instructions. For example, they might specify the amount of money to send and the location to make the request seem more legitimate. This information might be included in the initial email or a follow-up email after the target replies.

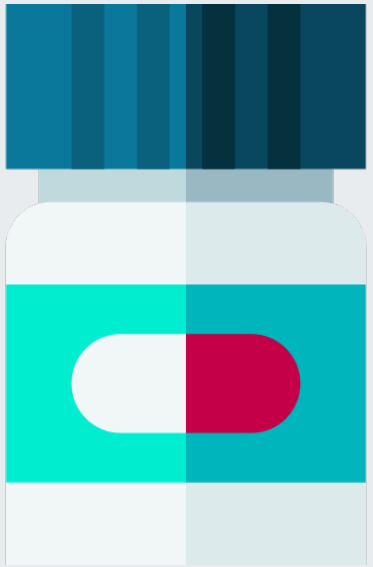


Example of a Business Email Compromise. *Source: PhishLabs*

...So You Can Spot the Signs

The Cost of a BEC Attack

- An example of what an organization DID NOT lose thanks to security measures in place.
- A local medical center reported that they received a phone call from a pharmacy to confirm a large order of prescription drugs, worth over $500,000.
- Upon investigation, it was determined the medical center had not placed that order, and it was in fact fraudulent.
- The pharmacy had called to clarify because the shipping address for the medical center was different from that which they had on record, but all the other information—like the Drug Enforcement Agency (DEA) ID number, doctor licenses, and pharmaceutical certificates—checked out.
- A malicious actor had compromised the medical center's credentials and was attempting to take out a line of credit with the pharmacy to purchase drugs.
- The pharmacy's act of calling the medical center to double-check the order saved them from losing $500,000 in prescription drugs and saved the medical center $500,000 being withdrawn from their account.
- The protocols in place were properly followed by the employee (i.e. calling to confirm when there is a change on an account) and the scam was stopped.



Prevention, Awareness, & Reporting

Preventing BEC Attacks

- **Set Network Access Rules:** Establish network access rules to limit personal device use and prevent information sharing outside the network's perimeter.
- **Update Infrastructure:** Ensure all applications, operating systems, network tools, and internal software are up-to-date and secure. These regular updates ensure that your defense mechanisms can handle the latest threats.
- **Anti-Phishing Protections:** Since BEC emails are a type of phishing, deploying anti-phishing solutions are essential to protecting against them. An anti-phishing solution should be capable of identifying the red flags of BEC emails (like reply-to addresses that don't match sender addresses) and using machine learning to analyze email language for indications of an attack.
- **Separation of Duties:** BEC attacks try to trick employees into taking a high-risk action (like sending money or sensitive information) without verifying the request. Implementing policies for these actions that require independent verification from a second employee can help to decrease the probability of a successful attack.
- **Labeling External Emails:** BEC attacks commonly try to impersonate internal email addresses using domain spoofing or lookalike domains. Configuring email programs to label emails coming from outside of the company as external can help to defeat this tactic.

- Simple Mail Transfer Protocol (SMTP), the protocol used to send emails, does not have authentication protocols built into it. Consider DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to fix this.
  - **DomainKeys Identified Mail (DKIM)** employs keys to prevent email spoofing by appending a signature to an outgoing email. Once the inbound server receives this email, the process checks the signature against the domain's public key. If they match, the process allows the email to go through, and if there is no match, it blocks the mail.
  - **Sender Policy Framework (SPF)** checks an email that comes into a mail server against the approved email senders for this sender's domain. The email is approved if there is a match between the approved mail exchanger and the actual one. If there is no authenticated match, the email is dropped to ensure it cannot reach employee inboxes.
  - **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** is an email authentication that verifies the authenticity of incoming emails. It helps prevent domain spoofing and ensures that emails originating from your domain are legitimate. It extends DKIM and SPF, enabling a domain owner to publish the domain's requirements for email authentication.

- Implement MFA across all email accounts within your organization.
  - When implemented across an organization, MFA reduces the risk of unauthorized access even if login credentials are compromised.
- Utilize a URL scanning service to ensure the validity of links.
- 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.
- Register all similar domain names that can be used for spoofing attacks.
- **Incident Response Plan:** Your organization 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.

Employee Awareness

- The first line of defense against business email compromise (BEC) is a well-informed workforce.
- Like all cyber threats that rely on manipulation, it only takes a single employee making a misguided decision to click on a malicious link or hand over personal information before dealing with a data breach that impacts your entire organization.
- By giving employees a heads-up on some common examples of business email compromise attacks, you provide them with the tools to spot manipulative phishing emails. You also reduce the chance of an attacker being able to trick your users into giving up sensitive information.

Train Your Employees:

- Conduct regular cybersecurity awareness training sessions to educate employees about the risks associated with phishing emails, social engineering, the importance of verifying sender information, and the reality of BEC attacks.
- Educate your employees about the five types of BEC attacks. Use phishing simulations to teach employees how to identify BEC and phishing attempts. Regular training facilitates better awareness, helping employees recognize, report, and respond to phishing attacks and malicious emails.

Reporting Business Email Compromise (BEC)

- If your organization falls victim to a BEC scam, it is important to act quickly:
  - Contact your financial institution immediately and request that they contact the financial institution where the transfer was sent.
  - Contact your local FBI field office to report the crime.
  - File a complaint with the FBI's Internet Crime Complaint Center (IC3).
  - Contact a Secret Service field office Cyber Fraud Task Force.

Report to the FBI's IC3

Reference Materials

References

- “5 Examples of Business Email Compromise Attacks,” Terranova Security. 30 June 2023. https://www.terranovasecurity.com/blog/examples-business-email-compromise
- “8 Phishing Types and How to Prevent Them,” BlueVoyant. N.d. https://www.bluevoyant.com/knowledge-center/8-phishing-types-and-how-to-prevent-them
- “14 Real-World Examples of Business Email Compromise (Updated 2022),” Tessian. 27 January 2022. https://www.tessian.com/blog/business-email-compromise-bec-examples/
- “19 Types of Phishing Attacks,” Fortinet. N.d. https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks
- “Business Email Compromise: What It Is and How to Prevent It,” National Cybersecurity Alliance. 18 December 2023. https://staysafeonline.org/resources/business-email-compromise-what-it-is-and-how-to-prevent-it/
- Benishti, Eyal. “The 3 Most Common Types of BEC Attacks (And What You Can Do About Them),” DarkReading. 7 January 2021. https://www.darkreading.com/vulnerabilities-threats/the-3-most-common-types-of-bec-attacks-and-what-you-can-do-about-them-
- “Business Email Compromise,” FBI. N.d. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/business-email-compromise

- “Business Email Compromise (BEC),” Check Point. N.d. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/business-email-compromise-bec/#:~:text=Business%20email%20compromise%20(BEC)%20is,sending%20money%20to%20the%20attacker
- “Business Email Compromise (BEC): Examples, Process, and Defensive Measures,” Perception Point. N.d. https://perception-point.io/guides/bec/business-email-compromise/
- “Business Email Compromise: In the Healthcare Sector,” Center for Internet Security. N.d. https://www.cisecurity.org/insights/blog/business-email-compromise-in-the-healthcare-sector
- Chin, Kyle. “19 Most Common Types of Phishing Attacks in 2024,” UpGuard. 18 January 2024. https://www.upguard.com/blog/types-of-phishing-attacks
- Esentire. “The Rise of QR Code Phishing Attacks and Best Practices for Interacting with QR Codes,” Esentire. 17 Nov 2023. https://www.esentire.com/blog/the-rise-of-qr-code-phishing-attacks-and-best-practices-for-interacting-with-qr-codes#:~:text=Scanning%20the%20QR%20code%20brings,directly%20with%20the%20threat%20actor.

- Gillin, Paul. “The history of phishing,” Verizon. N.d. https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/
- “History of Phishing,” Phishing. N.d. https://www.phishing.org/history-of-phishing
- Lenaerts-Bergmans, Bart. “WHAT IS BUSINESS EMAIL COMPROMISE (BEC)?,” CrowdStrike. 10 March 2023. https://www.crowdstrike.com/cybersecurity-101/business-email-compromise-bec/
- Protectera. “The Five types of Business Email Compromise (BEC) scams according to the FBI,” Protectera. 9 May 2022. https://protectera.com.au/types-of-bec-scams/
- “The Essential Guide to BEC (Business Email Compromise) Attacks,” Valimail. 25 July 2023. https://www.valimail.com/blog/essential-guide-to-bec-attacks/#:~:text=Why%20do%20bad%20actors%20use,to%20a%20fraudulent%20bank%20account

- Shantanu, Kumar. “Top Real-life Examples of BEC Attacks,” Threatcop. 23 June 2022. https://threatcop.com/blog/bec-attacks-examples/
- “Understanding Business Email Compromise,” United States Secret Service. N.d. https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident/BEC
- “What is quishing?,“ CloudFlare. N.d. https://www.cloudflare.com/learning/security/what-is-quishing/.
- “What is a Vishing Attack?,” Incognia. N.d. https://www.incognia.com/the-authentication-reference/what-is-vishing-attack-definition-examples-and-tips-to-protect-from-it#:~:text=Vishing%20attacks%20examples%20include%3A&text=The%20fraudster%20calls%20the%20victim,number%20to%20resolve%20the%20issue
- “What is business email compromise?,” Cisco. N.d. https://www.cisco.com/site/us/en/learn/topics/security/what-is-business-email-compromise-bec.html
- Wyro, Brad. “Four-Step Swindle: The Anatomy of a Business Email Compromise Attack,” MDaemon. N.d. https://blog.mdaemon.com/the-anatomy-of-a-business-email-compromise-attack

Questions

FAQ

Upcoming Briefing

- 6/13 – Healthcare Cloud Security

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV