Training Bulletin—Business Email Compromise

Trainer Notes

This bulletin raises awareness about a spear-phishing attack known as the Business Email Compromise (BEC). This social engineering attack has devastated many organizations in terms of cost and breach of sensitive information. Awareness and training is the first and best step toward preventing an attack on your business.

Business Email Compromise

BEC emails are a social engineering attack that usually rely on spear-phishing to trick its targets by impersonating a company executive or a vendor/partner and targeting a specific department within the organization. The request is usually for a wire transfer, invoice payment, or for W-2 information. Attackers rely on common communication patterns to make the request look like it's business-as-usual. BEC emails usually express urgency so that the targeted employee does not analyze the email and think before responding to the fraudulent request.

Talking Points

- Remind employees that cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.
- Make sure employees can spot a BEC email and are aware of the dangers of BEC and the impact an attack could have on your organization.
- Review and make sure employees understand how to recognize phishing and BEC emails and know to alert your IT department if they receive one.
- Review policies and procedures related to the types of requests in a BEC email —*i.e.* wire transfers, invoice payments, employee data requests.

CYBERSECURITY TRAINING BULLETIN

Social Engineering—Business Email Compromise

The Business Email Compromise (BEC) is a specific phishing attack that is disguised as an internal company or vendor/ partner email. The email may request a wire transfer, invoice payment, or for W-2 information. BEC emails usually express urgency in an attempt to dissuade you from analyzing the email and thinking before responding to the fraudulent request.

Here are some common examples of BEC:

CEO Scam:

An attacker sends an email posing as the CEO or another executive. The attacker claims to be handling confidential or urgent matters and requests a wire transfer to an account under his control. Attackers mimic the style of communication to make the email seem like business-as-usual. Many times organizations and finance departments fall victim to this type of attack.

Invoice Scam:

This scam usually relies on an established relationship between a business and supplier. An attacker poses as an employee of the supplier and sends a bogus invoice to the customer. The attacker requests funds to be wired for the invoice payment to their fraudulent account. Because the emails appear to be usual business requests, organizations fall for these attacks.

W-2 Scam:

This scam involves an attacker sending an email, once again posing as the CEO or another executive seeking employees' W-2 information. The email may look something like this:

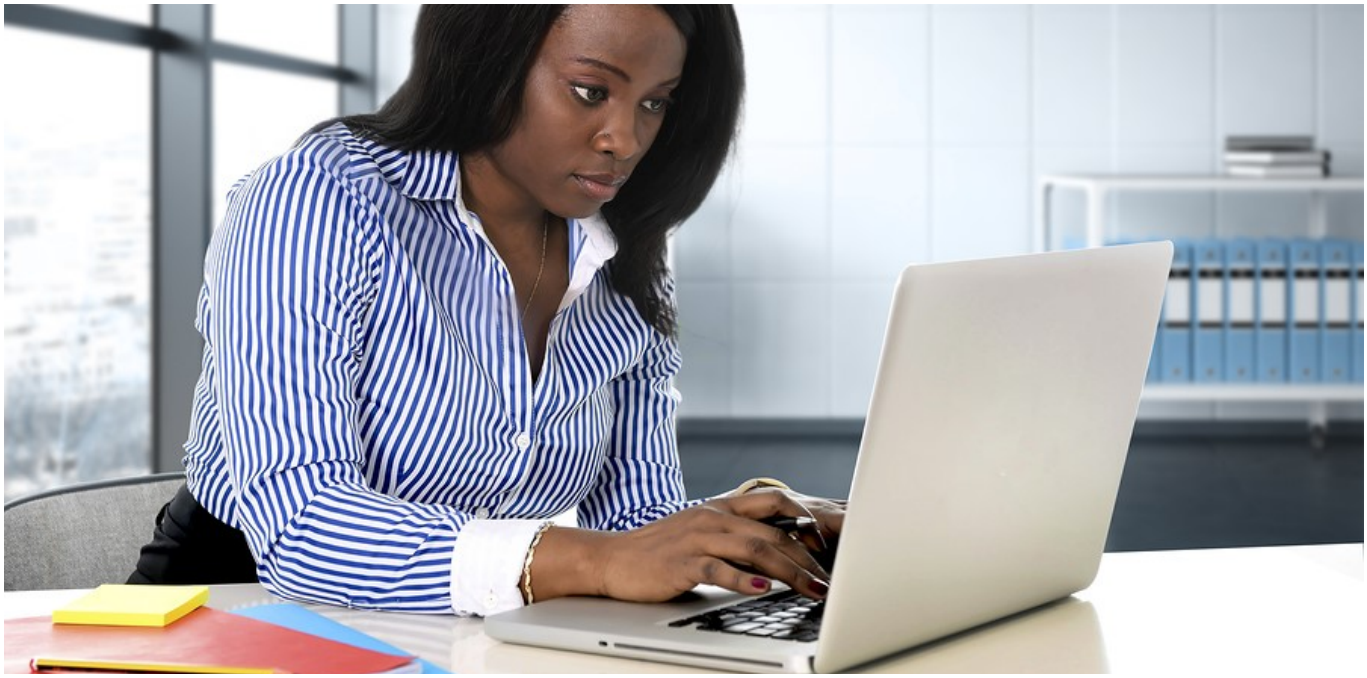
Kindly send me the individual W-2 and earnings summary for all company staff for a quick review.

Often, HR or payroll departments will comply with these requests and send the sensitive information to the attackers.

Best Practices:

Here are tips to defend against Business Email Compromise scams:

- Carefully analyze all emails, especially wire transfer requests and out of the ordinary requests from C-suite executives.
- Closely check the sender email address—often times the spoofed email will be one letter off.
- Confirm any request via telephone from a known number, not the one provided in the email request.
- Verify any changes in vendor payment by using a secondary sign-off by company personnel.



Training Bulletin Guidance—
Having a “Clean Desk” in the Workplace

Trainer Notes

A “**clean desk**” does not expose any sensitive or confidential information to those in its proximity and has sensitive or confidential information secured in a locked area and out of sight when not being used. An enforced clean desk policy is an important tool to ensure that all sensitive/confidential materials are **removed from a workspace and locked away** when the items are not in use.

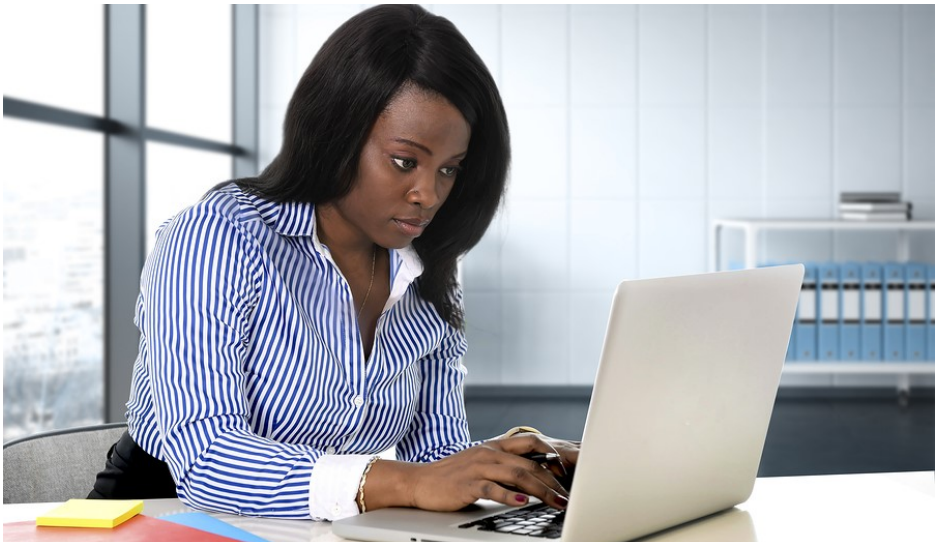
Implementing a clean desk policy will **reduce the risk of information theft, fraud, or a data breach** caused by sensitive information being visible in plain sight.

A clean desk policy should be in **writing and communicated to all employees** including during new and refresher employee training.

Consider having a manager check the office at the end of the day and confiscate or destroy any folders, papers or portable storage media an employee might have left out on their desk.

Talking Points

- Physical safeguards of sensitive information are as important as technical safeguards like passwords, multi-factor authentication and anti-virus software.
- Encouraging the use of digital versions of documents significantly reduces costs of paper, ink toner, and printer maintenance.
- Remind employees that cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.



CYBERSECURITY TRAINING BULLETIN

THE IMPORTANCE OF HAVING A “CLEAN DESK”

What is a “clean desk”?

A “clean desk” is a workstation that does not expose any sensitive or confidential information to those in proximity and that has the information secured in a locked area and out of sight when not being used.

Why is a “clean desk” important?

Having a clean desk is important because it significantly reduces the risk of information theft, fraud, or a data breach caused by sensitive information being visible in plain view.

Best Practices

What can I do to keep a “clean desk”?

Here are several ways you can have a clean desk.

- Secure all sensitive/confidential information in hardcopy or electronic form in your work area at the end of the day and when you are expected to be gone for an extended period.
- Lock or shut down your computer when the workspace is unoccupied or at the end of the day.
- Remove any sensitive/confidential information from your desk and lock in a drawer when the desk is unoccupied and at the end of the work day.
- Don’t post passwords on or under a computer or in any accessible location.
- Immediately remove printouts containing sensitive/confidential information from the printer.
- Shred documents containing sensitive/confidential information in official shredder bins or place in locked confidential disposal bins.
- Erase whiteboards containing sensitive/confidential information.
- Secure storage devices such as CDROM, DVD or USB drives in a locked drawer.

Training Bulletin Guidance—
Payment Cards and Your Employees

Trainer Notes

This bulletin raises awareness about handling payment card data and the PCI DSS. The Payment Card Industry Data Security Standard is a data protection standard developed by the Payment Card Industry for all businesses who handle payment card information. If your organization accepts or processes payment cards, your organization must comply with PCI DSS!

Noncompliance fees range from $5,000 to $100,000 every month until compliance issues are addressed. Even if you are compliant but experience a data breach, you can still be fined up to about $100 per cardholder whose data was compromised. That quickly adds up!

Talking Points

- Remind employees that cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.
- Hackers want your payment card data because they can sell it on the black market.
- Cardholder data should be secured from where it is captured at the point of sale and as it flows into the payment system. The best step is to not store any cardholder data!
- Remind employees that PCI DSS compliance is important, and that protecting payment card data should be a top priority in your cybersecurity program.

CYBERSECURITY TRAINING BULLETIN

Payment Card Guidance for Employees

What is PCI DSS?

The **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard is a data protection standard developed by the Payment Card Industry for businesses who handle payment card information. If your organization accepts or processes payment cards, your organization must comply with PCI DSS.

What steps can I take to maintain PCI DSS compliance?

- Where possible, try to limit payment card transactions to in-person "swipe" purchases using validated payment card processing equipment.
- If you take cardholder data over the phone, type the number directly into your point-of-sale (POS) system. Do not repeat the information if you could be overheard.
- Generally, refrain from writing cardholder data on paper. If you must, then:
    - protect the written information from unauthorized disclosure;
    - process the transaction as soon as possible; and
    - render the information unusable - destroy it in a shredder or use a permanent marker to black-out sensitive information.
- Never use cardholder data in email transactions.
- Do not allow unknown people to inspect, configure, repair or replace your POS equipment or computers.
- Inspect your POS equipment regularly for signs of tampering.
- Immediately report signs of potential POS compromise.

What are signs of potential POS compromise?

- New, unidentifiable equipment in POS area
- Open filing cabinet/drawer/safe used to store CHD
- Unusual/Unexplained transactions
- Lost keys or codes

Where can I learn more about PCI DSS?

Your organization should have policies, procedures and training that provide greater detail into expected practices.

The official website for PCI DSS is: http://www.pcisecuritystandards.org/

Remember, YOU are the first line of defense against payment card fraud!

Training Bulletin Guidance—
Mobile Device Security is Essential to a Robust Cybersecurity Program

Trainer Notes

Mobile devices provide great value to organizations in the form of increased productivity. But the increase in use of mobile devices leads to more lost and stolen devices and potentially significant data breaches. The healthcare industry is particularly plagued with consequences of lost and stolen mobile devices. For example, the University of Texas MD Anderson Cancer Center just paid over $4,000,000 because of three separate data breaches involving the theft of an unencrypted laptop and the loss of two USB thumb drives containing the unencrypted protected health information of patients. There are effective ways to reduce the occurrence of lost and stolen mobile devices and the resulting negative business consequences.

Organizations should first implement a comprehensive mobile device and media policy which outlines the proper use and storage of mobile devices. If a policy is already in place, organizations should review it and make sure it is adequate. A device and media policy should be in **writing and communicated to all employees** including during new and refresher employee training. Employee training of good mobile device habits is critical.

Other actions include encrypting all mobile devices, never leaving unattended your mobile device in a public area, securing the device out of sight and in your trunk if the device must be left in the car, and never store a password with the mobile device or its case.

Talking Points for You and Your Employees

- Data breaches are not just hackers electronically accessing your computer networks.
- Review the tips provided on the following page.
- Go over your mobile device management policy with new and existing employees.
- Remind employees that cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.

CYBERSECURITY TRAINING BULLETIN

THE IMPORTANCE OF MOBILE DEVICE (LAPTOP) SECURITY

Lost and stolen laptops and mobile devices directly affect an organization's bottom line.

The cost of a lost or stolen device is far greater than just the price of the device. Other costs include the value of the data on the device, fines and penalties from regulators, the reputational harm of a potential data breach and more.

So - keeping your laptops and mobile devices secure is very important!

Use these tips to keep your laptops and mobile devices secure!

- Laptops should always be stored in secure areas.
- Never leave laptop bags unattended in airports or other public facilities, and always use the hotel safe to secure equipment when you're not in the room.
- When traveling, keep laptops in the trunk and out of sight (if they must be left in the car).
- When flying, do not put laptops in your checked bags - secure your laptop in your carry-on bag.
- Don't keep your laptop passwords with the laptop or its case.

What if my laptop is lost or stolen?

If any device you use for work (including your own devices like a smartphone or laptop) is lost or stolen, **IMMEDIATELY** contact your supervisor, IT department or other individual as specified in your organization's mobile device management policy.

Cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.

Training Bulletin Guidance— Phishing

Trainer Notes:

Phishing emails remain the most common way hackers access your organization's environment.

Why? Because it's easier to get past humans than technology. Software manufacturers are releasing more secure software and it's increasingly difficult and expensive for hackers to exploit software vulnerabilities. On the other hand, it's cheaper (and easier) to simply trick a user into clicking a malicious link or opening an attachment in a phishing email to gain access into your organization's environment. Therefore, hackers are focusing on making their phishing emails harder to spot.

To help prevent successful phishing attacks on your organization, train your employees to spot a phishing email. Also, implement a social engineering awareness policy which, among other things, requires employees to take regular training on how to spot and report social engineering attacks like phishing emails. Organizations can also perform company-wide mock phishing exercises and conspicuously mark all external emails to aid employees in identifying a potential phishing email.

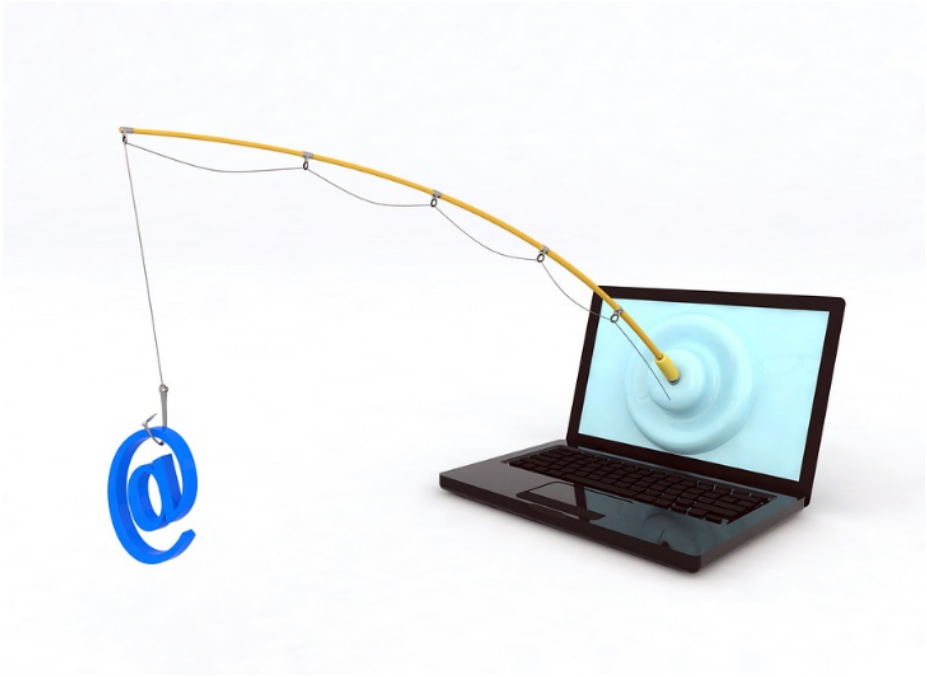
IMPORTANTLY, no one is perfect and even the most vigilant employees may fall victim to a phishing email. Enabling multi-factor authentication will help protect against account takeover even if credentials are compromised in a phishing attack.

Distribute the following page to your employees and discuss the below talking points to train them to recognize a phishing email!

Talking Points for Your Employees:

- Explain social engineering and phishing to your employees.
- Describe the damages that phishing emails can cause your organization.
- Tell employees the procedures to follow after receiving a suspected phishing email.
- Remind employees that cybersecurity is a team effort. Every employee counts, and participation from everyone is needed to maintain a good security posture.

CYBERSECURITY TRAINING BULLETIN



THE IMPORTANCE OF RECOGNIZING PHISHING EMAILS

Phishing emails remain the most common way hackers access your organization's environment. So – recognizing phishing emails is important!

Common Signs of a Phishing Email

- Your name is missing as an addressee in the email.
- Be suspicious of any email that requests your username/password or any personal information.
- Bad grammar and poor spelling.
- Short emails that threaten or otherwise create urgency to act.
- Hover your mouse over any website links and you should see the actual hyperlinked address. If the actual address is different from the displayed address, the message is likely malicious.
- Use common sense. If it's too good to be true, then it's likely not!
- Phishing emails are getting harder to spot. When in doubt, **ASK** before clicking on a link or opening an attachment.
- If you get an unusual email from a co-worker, call the sender and verify the email.

What if you get a phishing email?

Follow your company's policy on reporting phishing emails. If you don't know what to do, ask your supervisor or someone from IT. If you think you received a phishing email, report the email to the appropriate company personnel. Reporting a phishing email might prevent a co-worker from falling victim to the same email!

Training Bulletin Guidance—Ransomware

Trainer Notes

This bulletin raises awareness about ransomware. In 2017, ransomware attacks spiked. Awareness and training are critical steps to preventing a ransomware attack on your business.

Ransomware

Ransomware is a type of malware (malicious software) that 'kidnaps' your business data and holds it hostage until you pay a ransom. Ransomware holds your data hostage by encrypting it and preventing access to it. If the ransom is paid, the decryption key is sent to you to decrypt and recover your data. If the ransom is not paid, your data remains encrypted and unusable. Or, with some ransomware, you must pay the ransom within a certain amount of time otherwise the ransomware deletes your data.

Talking Points

- Remind employees that cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.
- Remind employees that malware attacks (like ransomware) are a real threat and every person and organization is a target.
- Employees can help prevent ransomware by understanding how to recognize phishing emails and knowing to alert your IT department if they receive one.

CYBERSECURITY TRAINING BULLETIN

Ransomware—Kidnapping Your Company Data

What is Ransomware?

Ransomware is a type of malware (malicious software) that 'kidnaps' your business data and holds it hostage until you pay a ransom. Ransomware holds your data hostage by encrypting it and preventing access to it. If the ransom is paid, the decryption key is sent to you to decrypt and ideally recover your data. If the ransom is not paid, your data remains encrypted and unusable.

Ransomware in the News

In 2017, ransomware attacks spiked with several attacks making the mainstream news. For example, WannaCry and NotPetya were two ransomware variants that made major headlines last year. WannaCry alone affected more than 300,000 organizations worldwide. Ransomware attacks are growing and employees play a big part in protecting an organization against ransomware.

How Does Ransomware Get on Your System?

Ransomware typically enters your network through outdated software, or, more commonly, when an employee responds to a phishing email by clicking on a link or opening an e-mail attachment containing malware.

Best Practices

Here are some ways you can help to defend against ransomware attacks.

- Recognize phishing emails. Don't open any attachments or click on any links in suspicious emails. Forward them to your IT department for verification. If you don't know how to recognize a phishing email – ask your IT department for help.
- If infected, IMMEDIATELY disconnect your computer from all networks and call your IT department.
- Always regularly back up business critical data and store backups disconnected from your network. You don't need to pay ransom if you have good backups!
- Keep all software on your computer up-to-date.