Click Wisely

A MINI TRAINING SESSION FOR LOSS PREVENTION

Quick Take on Data Security

Business Email Compromise and Misdirected Paymant Fraud

TRAINING OVERVIEW AND OBJECTIVES

Overview: Covers what business email compromise is and best practices to spot common scams, such as misdirected payment fraud.

Purpose:
- Reviews how to spot business email compromise and misdirected payment fraud attacks.
- Reviews best practices for verifying payment change requests.

Preparation:
- Read and become familiar with this Quick Take. *Change it as needed to reflect procedures and circumstances of your department.*
- Review applicable policies within your organization and update this Quick Take to reflect them.

Handouts:
- Quick Review of Data Security: Business Email Compromise and Misdirected Payment Fraud or Be Suspicious of Requests in Email digital image
- Quick Review of Data Security: Phishing and Social Engineering or Recognize and Report Phishing digital image *[Instructor Note: Provide if employees do not already have this.]*
- Entity's policy and procedures for payment practices

Misdirected Payment Fraud and Other Scams Often Come Through Email

Misdirected payment fraud is a bread-and-butter scam for thieves. Often the fraud is a phishing email, but it can also show up via text or phone call. Other business email compromise scams include requests to update or verify account information or passwords.

The emails typically look like they're coming from our known vendors or partners, which is intended to make it easy for us to fall for the scams. Despite this, we can use a few simple steps to help avoid becoming a victim.

Our IT professionals work to filter known or suspected scams from reaching our inboxes, but some slip through. It takes all of us doing our part to be on the lookout for scams. Please pay attention.

Why Is This a Big Deal for Us?

Local governments, such as [name of your organization], are easy targets, because our board agendas, summaries and minutes are publicly available, and they list our vendors, items and projects being purchased or bid, and the payment amounts. Criminals use this information to create emails that look legitimate and make a seemingly reasonable request.

Here are a few examples of business email compromise scams:

Example 1: The fraudulent email requests that we change how or where we make payments to a known vendor. So instead of remitting payment to our actual vendor, the money is rerouted to the perpetrator of the

fraud. Pretty much once the funds are released, we cannot claw back the misdirected payment. Think about how much some of our contracts amount to, sometimes in the hundreds of thousands of dollars, and you can understand that a significant amount could be at risk. *[Instructor Note: adjust example amount to make sense for your organization's vendor payments.]*

Example 2: A fraudulent email asks you to update or verify your log in credentials with our bank or other critical accounts or systems. If you follow the links to do this, you are giving the bad actors the keys to access our accounts or infiltrate our systems to do any number of bad things, including stealing money, acquiring sensitive data or deploying ransomware.

Example 3: A scammer spoofs the [entity's leader's name (e.g., finance officer, administrator, executive director)] email account, and then emails employees instructions to make a purchase or send money via a wire transfer. The scammer might even ask an employee to purchase gift cards, then request photos of the serial numbers.

How to Spot and Avoid a Scam

These best practices help us spot fraudulent requests for sharing account credentials or releasing funds:

- **Be suspicious of all unsolicited requests** to update or verify account credentials.
  - Typically, legitimate partners do not make these requests through email.
  - Be especially wary if the sender is pressing you to act quickly. This is a common tactic. Usually, nothing is so urgent that you can't take time to verify that the request is legitimate.
  - Look for tell-tale signs that a message is a phishing attempt before doing anything else. Examine spelling, the email address and link URLs. Slight differences from legitimate addresses are a hallmark of a scam. We have previously discussed how to spot a phishing attack, so you can review those tips on your own. *[Instructor Note: If you have not provided these tips previously, you may want to hand out the Quick Review on Data Security: Phishing and Social Engineering to staff.]*
- **Do not open attachments from senders you do not know** or have not verified. Be especially wary of attachments that have been forwarded to you. Hackers often use attachments to deploy malware, including ransomware, onto systems as soon as the file is opened.
- **Verify payment changes or purchase requests** before authorizing a change or buying anything.
  - Call the party making the request using a known, previously verified phone number. This is likely the one on file in our contacts system.
  - If reasonable, you could personally visit the person making the request to verify it. This may be best if the request is seemingly coming from an internal source, such as a department head, another employee or even me.
- **Do not verify using email**, especially do not reply to the email you think may be fraudulent. You would just be asking the criminal to validate his or her fraudulent request. One way you could use email to legitimately verify the request would be to start a new message to the requesting party and use the known, previously verified email address we have on file for him or her. This should prevent the message from delivering to the perpetrators of the theft attempt.
- Require the **payee** to **complete and sign a new direct deposit or ACH form** when a change is requested. Follow the verification technique we just discussed. Having a new form signed by the payee provides documentation that the change was authorized if an issue arises later.
- **Be suspicious of messages from Green Dot Bank**. This online bank is frequently used in misdirected payment fraud scams.
- **Do not make changes if you are not authorized to do so** for direct deposits, ACHs, fund transfers, account details and the like. We limit the number of people authorized to do this and have multiple steps for verification as part of our security protocol. If you receive a request for this type of action and you think it looks legitimate after going through the steps we just talked about, *[Instructor Note: Add your procedure steps here, such as "forward to an authorized person."]*
- **Investigate unusual requests**, ask questions and verify the authenticity of the request.

If you are unsure of any request that comes to you, please bring it to me. I would rather spend a few minutes verifying a legitimate request than you falling victim to a scam and having potentially hundreds of thousands of dollars of public funds lost to criminal.

DISCUSSION QUESTIONS

- What other ways can we identify and avoid potential scams that come through email?
- What other variations of these types of scams do you know or have seen?
- How do we report a suspicious or known fraudulent email?
- How else can we best maintain email and data security?

Business Email Compromise and Misdirected Paymant Fraud Session Planning and Review

Trainer	Training Date
Department(s)	

TRAINING GOALS

- Review how to spot a business email compromise and misdirected payment fraud attacks.
- Review best practices for verifying payment change requests.

RESOURCES

- Entity's policy and procedures for payment practices
- Business Email Compromise, Federal Bureau of Investigation

REVIEW

Did the training meet the stated goals?

[add comments here]

How can the training be improved?

[add comments here]

TRAINER COMMENTS

[add comments here]

Attendance Record

Training Session Business Email Compromise and Misdirected Payment Fraud

Trainer Training Date

Participant Name (printed)	Participant Signature