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.