Business Email Compromise - Phishing Discussion

Essential Planning LLC / Doran Independent Insurance
12/7/17

What is Social Engineering? The psychological manipulation of people into performing actions or divulging sensitive information.

What is Phishing? A form of Social Engineering. Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

What is Spear-Phishing? A phishing attempt directed at specific individuals or companies. Attackers may gather personal information about their target to increase their probability of success. This technique is by far the most successful on the internet today. Phishing is typically carried out by Email Spoofing.

What is Email Spoofing? The forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source.

What is Business Email Compromise (BEC)? The BEC is a social engineering attack that usually relies on spear-phishing to trick its targets- usually requesting a wire transfer, invoice payment, or for W-2 information.

> **CEO Scam:** An attacker sends an email posing as the CEO or another executive.
>
> **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.
>
> **W-2 Scams:** This scam involved an attacker sending an email once again posing as the CEO or another executive seeking employees' W-2 information.

Best Practices: Here are a few tips to defend against Business Email Compromise scams:

- Carefully analyze all emails, especially wire transfer requests and out of the ordinary requests.
- Closely check the sender email address- often times the spoofed email will be one letter off. ALWAYS HOVER.
- Stay updated on customers' habits and confirm wire transfer requests via telephone from a known number, not the one provided in the email request.
- Verify any changes in vendor payment location by using a secondary sign-off by company personnel.
- Don't take everything at face value. Before you open and click an email, go through these questions:
  Is the email from someone I recognize?
  Am I expecting the email?
  Are the requests of the email reasonable?
  Is the email using emotional gauges like fear or agency to entice an action?