Caltech

Cybersecurity Month - Week 2

THE ART OF PHISHING

What is Spoofing or Phishing?

Phishing scams attempt to trick people into providing passwords or other sensitive information by imitating legitimate websites and email messages. Phishing attempts have become increasingly prevalent and more targeted. IMSS security measures counter these attacks with IMSS managed email servers like Office 365 Exchange.

What to look for?

- Emails that appear to come from a high-ranking person at work, requesting payment to a particular account or providing sensitive information (i.e. passwords, banking information, social security no.)
- Emails that encourage you to act urgently. Be suspicious of words like 'send these details within 24 hours", or "you have been victim of a crime, click here immediately".
- Emails that mimic official Caltech emails, including logos and graphics. Pay close attention to the design and quality.

Protect Yourself

- IMSS will never ask you for your username and password
- Set up multi-factor (MFA) authentication on any account that allows it
- Do NOT click on links from unsolicited emails or texts
- Carefully examine the email address or website URL spelling
- Be careful with downloads. Never open email attachments from someone you don't know.

Other Phishing Variations

Vishing

Scams that happen over the phone, voicemail, or VoIP (voice over IP)

Smishing

Scams happen through SMS (text) messages

Pharming

Malicious code is installed on your computer to redirect to fake websites

THE ART OF PHISHING

continued

Be Cautious Online and with Social Media

Be careful with what information you share online or on social media. By openly sharing things like pets' names, schools you attended, family members' names, or your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.

Artificial Intelligence (AI) and Phishing

Miscreants leverage AI to impersonate organization members and conduct financial fraud by exploiting advanced technologies, such as deepfakes and AI-generated voice synthesis. Typically, this is how they do it:

Deepfake Emails

Attackers craft highly convincing phishing emails that mimic the writing style, tone, and communication habits of real organization members. This makes the fraudulent messages harder to detect, especially if they appear to come from senior executives or key decision-makers.

AI-Generated Voice Cloning

Attackers use AI voice synthesis to clone a target's voice, then make phone calls to employees or financial departments requesting urgent wire transfers or changes in payment instructions. The use of AI makes the impersonation indistinguishable from legitimate communications.

Personalized Phishing

AI can be used to scrape data from social media or internal communication channels. This allows attackers to customize phishing attempts to match the individual's interactions, preferences, and schedule. This level of personalization lowers the likelihood of suspicion and increases the success rate of fraud.

Business Email Compromise (BEC)

AI algorithms can analyze company patterns and behaviors. These assist attackers in sending targeted messages that fit the typical transactional behavior of the organization. This allows attackers to trick employees into sending payments to fraudulent accounts.

In all these cases, the AI-generated content created a sense of urgency or familiarity, leading victims to bypass usual checks, thus increasing the chance of successful financial fraud.

Next Week in the Series: Ransomware