Phishing Awareness Training

Protecting Yourself and Our Organization

By Garryella Noel

Introduction to Phishing

What is Phishing?

- Definition: The fraudlent practice of sending emails or other messages purporting to be from reputable companies in order it induce individuals to reveal personal information

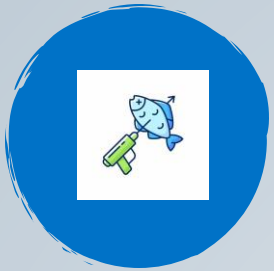
Common Methods

- Emails
- SMS/Smishing
- Phone calls

Types of Phishing Attacks

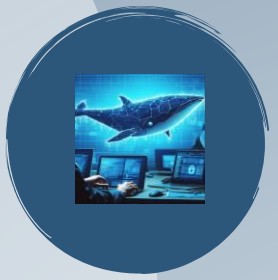
Email Phishing

A cyberattacker attempts to steal personal information by sending deceptive emails that appear to be from legitmate sources



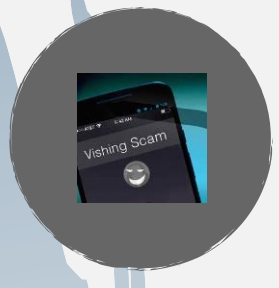
Spear Phishing

Are a more targeted approach that focuses on specific individuals and organizations



Whaling

A more sophisticated attack that is targeting high level executives



Vishing (Voice Phishing)

A scammer calls your phone in an attempt to steal information or money

Smishing (SMS Phishing)

Scammers that send deceptive text messages to trick victims into providing sensitive information

How Phishing Works

Email phishing is one of the most common phishing attacks where the primary aim is to trick individuals into divulging sensitive information like login credentials, credit card numbers, or to install malware on the victim's system.

Typical phishing scenario

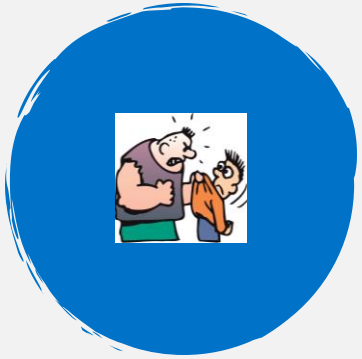
- Attacker sends a deceptive message
- Victim clicks on a link or opens an attachment
- Sensitive information is compromised

Recognizing Phishing Emails

What are the signs of a phishing email?

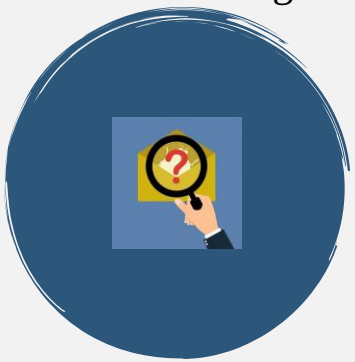
Unusual sender email address

A message from Amazon will come from amazon.com, not @clients.amazon.org



Urgent language or threats

"You need to make a payment, or your information will be sent to collection"



Suspicious links

When you hover your cursor above the link, it should reflect the website you're going to

Poor spelling and grammar

Official organizations will never send out emails with obvious spelling or grammatical errors

Case Study: Target Breach of 2013

Incident: In 2013, Target, a major U.S. retailer, suffered one of the largest data breaches in history, affecting over 40 million credit and debit card accounts. The breach began with a phishing attack on Fazio Mechanical, a third-party vendor providing Target with HVAC services. An employee at Fazio Mechanical fell for a phishing email, which allowed attackers to steal the vendor's network credentials. These credentials were then used to access Target's network, where the attacker installed malware on the point-of-sale (POS) systems of Target stores.

Impact on the Organization

- **Customer Data Compromise:** Hackers stole the payment card information of over 40 million customers, along with personal details of another 70 million
- **Financial Loss:** Target Spent over $200 million in legal fees, settlements, and upgrades to its security infrastructure

Lesson Learned

- **Vendor Management and Network Segmentation:** Target failed to adequately protect its network by allowing a vendor to access sensitive systems without sufficient security controls. Ensuring that vendors only have access to the minimum required systems and properly segmenting the network, would have mitigated the impact
- **Employee Training on Phishing:** The attack started with a phishing email, demonstrating that employees at all levels, including those of third-party vendors, need to be trained in recognizing phishing attempts and suspicious emails

Protecting Yourself From Phishing

1. Be Skeptical of Unsolicited Emails

- Avoid clicking on links or downloading attachments in unsolicited emails or messages from unknown senders.

2. Verify the Sender’s Email Address

- Always check the sender's email address, not just the display name. Attackers often use email addresses that look similar to legitimate ones, with slight alterations (e.g., support@paypa1.com vs. support@paypal.com).

3. Hover Over Links

- Before clicking on a link, hover over it to see the actual URL. Ensure that it directs to a legitimate and secure website. Secure websites start with "https://" and often show a padlock symbol.

4. Use Multi-Factor Authentication (MFA)

- Enable MFA wherever possible. Even if an attacker gains access to your password, MFA adds an extra layer of security, requiring additional verification (e.g., via a mobile device).

Continued

5. Keep Software Updated

- Regularly update your operating system, browsers, and other software to ensure they have the latest security patches. Phishers may exploit vulnerabilities in outdated software.

6. Don’t Share Personal Information via Email

- Legitimate organizations will never ask you to provide sensitive information (e.g., passwords, Social Security numbers) via email. Be cautious of emails requesting such details.

7. Use Strong, Unique Passwords

- Use complex passwords that combine letters, numbers, and symbols. Avoid reusing passwords across multiple sites.

Reporting Phishing Attempts

What to do if you suspect phishing

Look for Red Flags in the Message

- Phishing emails often have poor grammar, urgent request for sensitive information, or unusual request. Be wary of any messages that seems out of place or overtly urgent

Report the Email

- If you're part of an organization, report the suspected phishing email to your IT or security team. If it's personal, most email providers offer a "Report Phishing" option that can help flag the message to prevent further incidents

Update Security Settings and Scan Your Device

- Ensure your antivirus software is up-to-date and run a full scan of your device to detect any potential threats. Additionally, update your passwords and enable multi-factor authentication (MFA)

Tools and Resources

1. Avanan

- Avanan offers anti-phishing software for cloud-hosted email, tying into your email provider using APIs to train their AI using historical email. The service analyzes not just message contents, formatting, and header information, but evaluates existing relationships between senders and receivers to establish a level of trust. Additionally, Avanan can detect suspicious messages in Teams or Slack, both emerging attack vectors.

2. Barracuda Email Protection

- Barracuda Email Protection is another tool that leverages mail provider APIs to protect against phishing as well as business email compromise (BEC). Barracuda's offering protects against a range of phishing variants, from spear phishing to impersonation to zero-day phishing attacks. Because compromised email accounts tend to lead to more phishing attempts or further account-based attacks, Barracuda's focus on minimizing further damage as a result of a successful phishing attempt has more value than relying solely on prevention. Barracuda also provides brand protection and domain fraud prevention through DMARC analysis and reporting.

3. BrandShield

- BrandShield focuses exclusively on protecting your corporate brand and that of your executives. Identifying phishing attacks (through email, social media, or other mediums) which leverage your brand or the names of your executives is just one component of BrandShield's portfolio. BrandShield also monitors the internet for rogue websites using your brand as well as marketplaces like Amazon where physical counterfeits of your products could pop up for sale.

Conclusion & Key Takeaways

1. Recognize Common Signs of Phishing:

Suspicious Emails/Links: Be cautious of unexpected or unsolicited emails, especially those asking for personal information or financial details.

Urgency and Fear Tactics: Phishing emails often create a sense of urgency, claiming your account will be closed, or you need to act fast.

2. Verify Sources:

Direct Contact: If you're unsure about an email, don't click on links or download attachments. Instead, contact the company directly using official communication channels.

Check Email Domains: Legitimate companies usually use official domains. Watch for slight variations like “company-security.com” instead of “company.com.”

3. Don’t Share Sensitive Information:

- **No Requests for Personal Data:** Reputable organizations will never ask for passwords, social security numbers, or financial details via email.
- **Secure Sites:** Only input sensitive information on secure websites (look for "https" in the URL).

4. Stay Updated on Latest Threats:

- **Employee Training:** Regularly educate yourself and colleagues on phishing techniques.
- **Phishing Simulations:** Participate in or run internal phishing tests to help staff identify phishing attempts.

Q&A

Garryella Noel

718-465-5090

noelgarryella798@gmail.com