Familiarize yourself with phishing attacks

Human Resources & Marketing

What is phishing?

Phishing is a form of social engineering and a scam where attackers deceive people into revealing sensitive information or installing malware such as viruses, worms, adware, or ransomware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim navigates the site, and transverses any additional security boundaries with the victim. As of 2020, it is the most common type of cybercrime, with the FBI's Internet Crime Complaint Center reporting more incidents of phishing than any other type of cybercrime

Learn to spot phishing emails

To spot a phishing email, look for signs such as generic greetings, poor spelling and grammar, mismatched email domains, and urgent calls to action that pressure you to click links or provide personal information. Always verify the sender's email address and avoid clicking on suspicious links or attachments.

Phishing emails will typically contain at least one of the following telltale signs:

1. Asks for Sensitive Information
2. Uses a Different Domain
3. Contains Links that Don't Match the Domain
4. Includes Unsolicited Attachments
5. Is Not Personalized
6. Uses Poor Spelling and Grammar
7. Tries to Panic the Recipient

How do we stop getting phished?

1. Be Skeptical of Unsolicited Communications:

- **Emails:** Be cautious of emails from unknown senders, especially those asking for sensitive information or urging immediate action.
- **Links:** Avoid clicking on links in unsolicited emails or messages. Hover over the link to see the actual URL before clicking.
- **Attachments:** Don't open attachments from unknown or unexpected sources.

How do we stop getting phished?

2. Verify the Source:

- **Sender's Email Address:** Check the sender's email address carefully. Phishers often use addresses that look similar to legitimate ones.
- **Direct Contact:** If you're unsure about an email or message, contact the company or individual directly using a known and trusted method.

How do we stop getting phished?

3. Look for Signs of Phishing:

- **Spelling and Grammar:** Phishing emails often contain spelling and grammatical errors.
- **Urgency:** Be wary of messages that create a sense of urgency or fear, pressuring you to act quickly.
- **Generic Greetings:** Legitimate companies usually address you by your name, not generic terms like "Dear Customer."

How do we stop getting phished?

4. Use Two-Factor Authentication (2FA):

- **Extra Layer of Security:** Enable 2FA on your accounts to add an extra layer of security. Even if your credentials are compromised, the attacker would need the second factor to access your account.

How do we stop getting phished?

5. Educate Yourself and Others:

- **Training:** Participate in cybersecurity awareness training to stay informed about the latest phishing tactics.
- **Awareness:** Keep your family, friends, and colleagues informed about phishing and how to avoid it.

How do we stop getting phished?

6. Check Website Security:

- **HTTPS:** Ensure the website uses HTTPS, indicating a secure connection. Look for the padlock icon in the address bar.
- **Domain:** Verify the website's domain carefully, as phishers often create look-alike domains.

How do we stop getting phished?

7. Use Anti-Phishing Tools:

- **Browsers:** Utilize built-in anti-phishing tools in browsers like Chrome, Firefox, and Edge.
- **Security Software:** Install and update reputable antivirus and anti-phishing software.

How do we stop getting phished?

8. Report Suspicious Activity:

- **Phishing Emails:** Report phishing emails to your email provider and the company being impersonated.
- **Incident Reporting:** Use the Anti-Phishing Working Group (APWG) or your country's cybersecurity agency to report phishing attempts.

How do we stop getting phished?

9. Keep Software Updated:

- **Updates:** Regularly update your operating system, browsers, and applications to patch vulnerabilities that phishers may exploit