Understanding and Responding to Phishing Threats

Phishing attacks have become a pervasive threat in today's digital landscape. Threat actors use deceptive tactics to manipulate individuals into divulging sensitive information or performing actions that compromise their security. Recognizing the signs of phishing and understanding how to respond is essential to protect against such threats.

WHAT TO DO IF YOU SUSPECT PHISHING

Encountering a potential phishing attempt can be unsettling, but maintaining composure and responding cautiously is key to minimizing the associated risks. Here's a guide on how to handle suspected phishing incidents:

- **Do not panic:** Maintain composure and avoid hasty actions; threat actors create a false sense of urgency to pressure you to act
- **Do not click on any links** because they may redirect you to fraudulent websites or initiate downloads of malicious software
- **Do not download any attachments;** they may contain malware or ransomware that could infect your device
- **Do not share personal information:** Safeguard sensitive details from phishing attempts; personal information can be used by threat actors to commit identity theft, fraud, or other malicious activities
- **Do not reply or forward:** Avoid escalating the impact of the phishing attack
- **DO contact your IT department:** Promptly report the incident for investigation and guidance

IDENTIFYING COMMON PHISHING SCAMS

Understanding the variety of phishing scams can help individuals recognize and mitigate these threats. Common phishing schemes include:

- **CEO / Business Impersonation:** Phishers pose as company executives or trusted business entities to trick employees into divulging sensitive information or initiating wire transfers
- **Account Lockout / Password Reset:** Fraudulent notifications requesting immediate password changes or claiming account lockouts to steal login credentials
- **Tech Support Scams:** Phishers impersonate technical support, coercing individuals to provide remote access to their systems or install malware under the guise of offering technical assistance

IDENTIFYING COMMON PHISHING SCAMS (continued)

- **Bank Alerts and Financial Scams:** Fraudulent notifications pretending to be from financial institutions, aiming to extract sensitive financial details or encourage fraudulent transactions
- **Tax Refund and Finance-Related Scams:** False notifications about tax refunds or financial opportunities to deceive individuals into sharing financial or personal information
- **Healthcare Announcements:** Fake notifications related to health information, insurance, or medical services to deceive individuals
- **Social Security Alerts:** Phishers impersonate government agencies or offer false security alerts to extract personal information
- **Gift Card Schemes:** Deceptive requests for gift card purchases under the disguise of business transactions or emergencies
- **Shipping Notifications and Parcel Scams:** False notifications of package deliveries or shipment issues aiming to extract personal or financial information
- **Survey and Employment Opportunity Scams:** Deceptive invitations to participate in surveys or fraudulent employment opportunities that aim to extract personal or financial information

CONCLUSION

Phishing remains a significant threat in today's interconnected world. Recognizing the signs of phishing attacks and understanding how to respond is pivotal to staying secure in an increasingly digital world. By being vigilant and informed, individuals can reduce their vulnerability to such deceptive tactics and protect their sensitive information.

ADDITIONAL RESOURCES

- Recognize and Report Phishing by CISA
  - cisa.gov/secure-our-world/recognize-and-report-phishing
- Small Business Cybersecurity Corner by NIST, Revised November 18, 2019
  - nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

ABOUT ADVANCED

For more than 40 years, Advanced has been a leading provider of comprehensive IT solutions: creating innovative networks, implementing comprehensive cybersecurity initiatives, and delivering exceptional IT support. Our proactive approach to trends and threats drives the development of scalable solutions to help business stay ahead in an ever-evolving technology landscape.

As always, Advanced is proud to be here for all your security needs. Reach out now (advance@actweb.com) to determine how you can improve your security posture and keep your business running smoothly.