www.prismrisk.gov

RISK SIMPLIFIED

RESOURCES

Cybersecurity and Infrastructure Security Agency

Synoptek- Managed IT Services

KnowBe4

QUESTIONS

Email PRISM Risk Control
or call 916.850.7300

Cyber Smart: Phishing

by Scarlett Sadler

Phishing is a type of social engineering where a cyber threat actor pretends to be a trusted individual or organization in order to deceive an employee into revealing sensitive information or granting access to their network. Employees represent the primary vulnerability to phishing attacks within an agency, and human factors in cybersecurity encompass situations where human errors lead to successful data or security breaches. They constitute the most susceptible element in safeguarding the security of any Information Communication Technology infrastructure and introduce the highest levels of risks and threats to an agency. Public agencies can experience various forms of phishing designed to exploit these vulnerabilities within the agency. Since there are various forms of phishing, it is important for public agencies to understand the types and ways to protect their agency. Some common types of phishing that a public agency may experience include:

- **Email Phishing:** Public agency employees often receive phishing emails that appear legitimate but are actually fraudulent. These emails may mimic official communication from trusted entities or individuals, such as internal departments, partners, or vendors. They typically contain malicious links or attachments that, when clicked or downloaded, can lead to data breaches, malware infections, or credential theft.
- **Spear Phishing:** In spear phishing attacks, threat actors customize their phishing attempts to target specific individuals within a public agency. They gather information about the targeted employees from publicly available sources or through social engineering techniques. By personalizing the attack, attackers increase the chances of success, as the phishing emails appear more genuine and trustworthy.
- **Phone-based Phishing (Vishing):** Public agency employees may receive fraudulent phone calls from individuals claiming to be representatives of trusted organizations or even internal departments. These callers attempt to extract sensitive information or persuade employees to perform certain actions, such as disclosing passwords or granting remote access to their systems. Vishing attacks rely on social engineering techniques to manipulate employees over the phone.
- **Smishing:** Smishing refers to phishing attacks conducted through text messages (SMS). Public agency employees can receive text messages that appear to be from legitimate sources, such as government

entities or service providers. These messages often contain links that, when clicked, direct the recipient to malicious websites or prompt them to provide sensitive information.

There are several measures that public agencies can take to prevent and mitigate the effects of phishing attacks. These include:

- **Develop Strong Policies and Procedures**
  - Create and enforce policies that address social engineering risks, such as strict access controls, password management, and data handling guidelines.
  - Limit access privileges to only what employees need to perform their tasks, reducing the potential for unauthorized access or manipulation.
- **Employee Training and Education:**
  - Periodically conduct security awareness training sessions that educate employees about the various social engineering techniques mentioned above.
  - Teach employees to recognize suspicious behaviors, such as unsolicited requests for sensitive information or unexpected changes in procedures.
  - Reinforce the importance of confidentiality and the need to verify identities before sharing sensitive information or completing requests.
  - Provide regular refresher training sessions to keep employees informed about emerging social engineering tactics and reinforce best practices.
  - Conduct periodic phishing simulation exercises to assess employee readiness and identify areas for improvement.
- **Strengthen Authentication Practices**
  - Require employees to use Multi-Factor Authentication for accessing sensitive systems and resources, adding an extra layer of security beyond passwords.
  - Implement and enforce policies that promote the use of complex, unique passwords and regular password changes.
  - Maintain an updated inventory of user accounts and regularly review and revoke unnecessary or inactive accounts.

A successful phishing attack on a public agency can have devastating consequences. Cyber threat actors can acquire valuable data, including personal information, financial records, and confidential documents pertaining to the agency. To mitigate this risk, it is crucial to establish robust policies and security measures while fostering a culture of continuous education and awareness among employees. Keeping employees well-informed can reduce the likelihood of an employee falling victim to a phishing attempt. For questions regarding phishing or cyber security, please contact Risk Control.