States Confront the Cyber Challenge

Q&A: Phishing

What is phishing?

Phishing refers to the criminal practice of using fraudulent emails to trick unsuspecting victims into disclosing sensitive information or downloading malicious software (malware). Phishing messages are usually designed to resemble a standard message from a trusted source, such as a school or a bank. Unlike general phishing scams, *spear phishing* campaigns target specific individuals with highly tailored emails. For example, an attacker may generate an email address resembling an account owned by the victim's mother, containing a computer virus masquerading as an attachment labeled "Vacation Photos." Social media provides hackers with information they can use to craft incredibly convincing phishing emails.

Why do criminal actors use phishing?

Phishing makes life easy for hackers. It is popular among foreign militaries and everyday criminals alike because it offers access to well-protected computer systems and data without the need to use far more complicated hacking tools. A phishing victim who carelessly chooses to download an unknown attachment or discloses private login information is essentially defeating their own security measures on behalf of the attacker. Hackers can then leverage their newfound access to commandeer the victim's computer and steal financial data or embarrassing personal information. They can also use the victim's email account to send additional phishing emails to new targets, spreading the damage.

How is phishing deployed against the public sector?

- An unknown actor gained access to millions of tax records held by South Carolina after an employee in the Department of Revenue executed malware hidden in a phishing email.
- Unknown hackers stole login credentials belonging to Arizona lawmakers and their staff by sending emails that appeared to originate from the Arizona's human resources department.
- In Indiana, phishers posing as IRS agents during tax season gained access to citizens' personal information without having to exploit any software flaw.
- A phishing attack against a public water utility in Michigan forced the company to shut down some of its networks as a precaution against compromise of the utility's control systems.

How can my state defend against phishing?

Basic cyber hygiene can prove very effective against phishing scams. *Most* phishing attempts will fail if their human targets do not open emails from strangers, click on suspicious links, or download attachments. State agencies should prioritize defenses that reduce the risk of these three events. Training is an indispensable component, as are simple technical measures (e.g., disabling web links in emails). Such security controls should be completely locked down—only a select few employees should have the power to change them.

It is also vital to ensure that all employees promptly report any phishing attempts, especially when they fall prey to one. Agencies should cultivate an environment that encourages reporting of all security incidents.