Combating spear phishing attacks

Cyber insights for the federal government

Today's reality:

- Spear phishing continues to be a concern for the federal government. Back in 2006, the Joint Task Force-Global Network Operations warned Department of Defense (DOD) users that everyone in DOD is a target and attempts have been made against all ranks in all services in all geographic locations. As evidenced by recent events, the spear phishing threat remains today.
- Agencies that fail to invest in preventative measures and do not have a rapid response plan in place are especially vulnerable to attacks by cyber criminals.
- Agencies need to educate employees about the dangers of phishing and spear phishing and train them on how to identify and respond to incident.

How to protect against this more sophisticated and dangerous form of phishing

What's at stake?

The need for sound security practices and controls is imperative to help protect against a growing swell of sophisticated cyber threats. Targeted attacks, including those perpetrated via e-mail, such as spear phishing, have become commonplace. In fact, spear phishing attacks now account for 91 percent of all modern attacks.[1] Additionally, it is almost certain that these attacks will increase in frequency and sophistication as agencies expand the use of digital assets and unstructured data.

Organizations stand to lose far more than their intellectual property in the aftermath of a spear phishing attack. Damage to reputation and public trust can be just as devastating as theft of property and secrets.

Phishing and spear phishing – a closer look

Recent events illustrate the prevalence of attacks within the federal government. For example, a former U.S. Department of Energy (DOE) employee plead guilty in February 2016 to attempting a spear phishing attack that targeted DOE employee e-mail accounts.[2]

Phishing: A deceptive process by which a cyber criminal attempts to steal your online identity—such as your username, passwords, personal identity number, credit card information, or bank details—by masquerading as a person or organization you trust.

Typically carried out via e-mail, instant messaging, and/or text messages, the phishing correspondence usually appears to come from a legitimate party with whom you may have a relationship and may include an agency's seal. Phishing e-mails or messages usually contain a

[1] http://www.firmex.com/blog/spear-phishing-whos-getting-caught/

[2] https://www.justice.gov/opa/pr/former-us-nuclear-regulatory-commission-employee-pleads-guilty-attempted-spear-phishing-cyber

link to an authentic-looking Web site or e-mail address, and ask you to provide your confidential information. As these e-mails and Web sites evolve and become more authentic looking, more people are falling for phishing attempts and are providing this information to scam artists.

Spear phishing: A more targeted and sophisticated form of phishing. Unlike standard phishing schemes that use mass e-mails, spear phishing schemes target individuals that fit a certain profile. For example, they may only target high-ranking employees of a governmental agency, or users of a specific site. Further more, the request for information may appear to come from a colleague working at the same agency.

The goal of these scam artists is to lure recipients into divulging sensitive information about themselves and/or their organization. Sophisticated attackers do extensive research on their targets prior to sending out e-mails, so they not only look realistic, but the information requests seem plausible and do not raise suspicion. This added element of social engineering and relevance makes a spear phishing message particularly effective and dangerous.

Recent cyber attacks in the news highlight danger

While many breaches start with spear phishing attacks, data stolen during an attack can be used for subsequent phishing attacks. For example, the U.S. Office of Personnel Management (OPM), which manages the federal civil service, sustained a data breach in April 2015 that impacted personnel records of 21.5 million people, including current, former, and retired federal employees and contractors. The attackers accessed the background investigation databases and stole sensitive information, including Social Security Numbers, birth dates, addresses, fingerprints, and other identification details.[3]

Unfortunately, the compromised OPM data may have a ripple effect. The cyber criminals may be able to use this information to breach additional targets by sending highly customized e-mails, fraudulent letters, or even making phone calls to organizations and individuals.

10 steps to protect against cyber attacks

These cases should serve as a loud wake-up call to organizations as to just how difficult it is to prevent cyber attacks, especially those with social-engineering aspects. A single employee can inadvertently cause a serious breach that could have a cascading effect throughout an organization as well as its customers and clients.

There are, however, several proactive steps an

[3] http://federalnewsradio.com/opm-cyber-breach/2015/07/opm-says-21-5-million-affected-by-second-cyber-breach/

agency can take that may minimize the likelihood of a successful attack. Agencies must understand that a sound cybersecurity program requires maturity across people, process, and technology, as no one element alone is sufficient:

People

1. **Adopt a strategic vision and communicate it –** An organization's leadership must adopt a clear, strategic vision of how to protect and secure critical and sensitive information assets across people, process, and technology. This message needs to be communicated throughout the agency and continually reinforced.
2. **Educate and train all employees –** It is critical to provide ongoing training and education for all employees, including executives, in order to increase cyber awareness. Remember, it only takes one employee opening an attachment in a targeted e-mail message to open the door for cyber criminals and potentially compromise an agency's network.

Process

3. **Develop a data governance strategy –** Organizations need to develop a strong data governance regime that includes the classification and monitoring of critical or sensitive data.
4. **Perform simulated attacks –** Organizations should perform simulated spear phishing attacks to measure the effectiveness of their end-user education and information security response. These simulations can help an organization identify individuals and groups that require additional training and help to identify gaps in security controls and policies.
5. **Develop incident response planning –** By developing an incident response plan that defines key roles and responsibilities as well as internal and external coordination steps throughout the incident life cycle, an organization can prepare itself for potential cyber attacks. In addition, the organization should test its plan periodically to help ensure that personnel are prepared to respond to a real-time incident and that the planned steps are effective.
6. **Perform periodic audits –** Periodic, thorough audits of accounts used to access critical systems within their environment should be performed. Similarly, they should remove unused and unnecessary accounts to help reduce the number of potential avenues for an attack to occur.

Technology

7. **Segment networks –** In order to reduce the overall impact and breadth of a successful security breach, organizations should design and configure their networks by segmenting critical systems and data stores.
8. **Update patching and antivirus programs –** Effective patch management and up-to-date applications, including Web browsers, are critical components of an effective defense against spear phishing attacks. An organization should confirm that its antivirus programs, operating system patches, and application patches are up-to-date in order to increase its overall security posture and protect against cyber attacks.
9. **Implement two-factor authentication –** Organizations should implement two-factor authentication for all critical systems to help protect sensitive data from attackers with stolen credentials. For example, in order for someone to access an organization's compensation or confidential personnel data, he or she would need to have both a physical token, e.g., a card, and a password or security code.
10. **Adopt system monitoring and access control technology –** Organizations should adopt the most up-to-date technologies to help detect and prevent potential threats by monitoring network traffic and controlling access to critical systems. Organizations should implement a layered security approach comprising both intrusion detection and intrusion prevention systems to monitor network traffic at the perimeter and within the firewall.

About KPMG Cyber

KPMG Cyber assists global organizations in transforming their security, privacy, and continuity controls into business-enabling platforms while maintaining the confidentiality, integrity, and availability of critical business functions. The KPMG Cyber approach strategically aligns with our clients' business priorities and compliance needs.

Contact us

Greg Bell
Principal, KPMG Cyber – US Leader
T: 404-222-7197
E: rgregbell@kpmg.com

Edward L. Goings
Principal, KPMG Cyber – Digital Response Services Lead
T: 312-665-2551
E: egoings@kpmg.com

Ronald E. Plesco
Principal, KPMG Cyber – Cyber Investigations Lead
T: 717-260-4602
E: rplesco@kpmg.com

Tony Hubbard
Principal, Federal Advisory
T: 703-286-8320
E: thubbard@kpmg.com

Ken Adams
Director, Federal Advisory
T: 703-286-8102
E: kennethadams@kpmg.com

kpmg.com/us/forensic

KPMG Cyber 24 x 7 Hotline 855-444-0087

kpmg.com/socialmedia