InfosecPartners
CYBERSECURITY

#SECURITYMANAGED

TEST YOUR ABILITY TO SPOT ATTACKS

PHISHING EXPOSURE ASSESSMENT

People are still the weak link...

No one likes to be fooled but people are still the weak link in an organisations security, falling for phishing even more often than before leading to security breaches and fraud.

Social engineering in its basic form is simply to dupe or trick someone into doing something they would not otherwise do, with tactics taking a myriad of forms including:

- Pretexting. The attackers present themselves as someone else in order to obtain private information
- Elicitation. The subtle art of extracting information from a subject via conversation.
- Baiting. The attacker plants infected media in victim areas.

A phishing attack uses social engineering in the form of a correspondence which attempts to get the recipient to take the bait in the form of an attachment or embedded link. It is important to note that 'pretexting' via email (a back-and-forth dialogue leveraging an invented scenario to gain a certain end) and a phishing email are similar but not the same. In the case of a pretexting email, the criminal is primarily purporting to be someone they are not, usually within the victim organisation.

Anatomy of a phishing attack

Typically the user clicks on a link or attachment, malware is installed on their device, and a foothold is gained by the attacker. There are still cases where the phishing email leads users to fake sites - used to capture user input - but the majority of phishing cases feature phishing as a means to install persistent malware. The victim opens the email, clicks on the attachment containing malware and what happens next is dictated by the end goal of the attacker.

What is Phishing?

- A form of social engineering that uses email or malicious websites (among other channels) to solicit personal information from an individual or company by posing as a trustworthy organization or entity.
- Phishing aims to trick the recipient in opening an attachment or clicking a link.
- Flash remains a security risk. JavaScript is being used to conceal malware hidden in Flash, making it harder to find and analyse.
- Attacks based on Java, which held a strong lead as the most widely used attack vector, have gone down whilst Silverlight attacks are on the rise.
- PDF files continue to be used to distribute malware, too, indicating that email-based phishing is still effective.
- Malvertising from malicious browser add-ons is also on the rise.

PHISHING EXPOSURE ASSESSMENT: Test your ability to spot attacks

PHISHING EXPOSURE ASSESSMENT

Safely simulate phishing attacks to test the security awareness of your staff and evaluate your network security infrastructure's ability to reflect attacks.

With the rise in instances of phishing and cyber fraud, and the costly damages and loss seen by victims of ransomware and Business Email Compromise, there is a need to test your organisations' susceptibility to social engineering attacks in a similar way in which you should test your network security defences with penetration testing.

The assessment identifies email addresses related to the organisation that are exposed on the Internet and easy to find for cyber criminals. These email addresses can in turn be used to launch social engineering, spear phishing and ransomware attacks against the business. These types of attack are hard to defend against unless users have next-generation security awareness training. The more email addresses and identities that are exposed, the larger the phishing attack surface is and the higher the risk.

On collecting the email addresses and identities, targeted phishing campaigns are simulated, recording the delivery, open and click-through activity of each user. Executives and staff in key positions are also targeted and 'pretexting' is employed to measure susceptibility to cyber fraud, indicating any weaknesses in account control or authorisation processes. In addition, this tests the security infrastructure's capability to respond to viruses, spyware and spoofed emails.

An additional component of the assessment involves carrying out security research to identify and personal or company sensitive information that has leaked onto the Internet or Dark Web.

Are you 'Once bitten, Twice Shy' or a 'Repeat Offender'?

Frequency and repetition is essential in effective security testing which is why our Phishing Exposure Assessment is recommended not just as a one off exercise, but carried out over a prolonged period. This is in order to get a measure of any improvement in security awareness and the infrastructures ability to automatically identify and defend against attacks, or alternatively identify individuals who repeatedly fall victim to the simulated attacks.

There's no time to wait.

Phishing and social engineering threats are at an all-time high with more businesses suffering now than ever before. Cyber criminals are reaping the benefits from poor security awareness as shown by the rise in cyber fraud including Business Email Compromise and Ransomware. Security technology is not enough – better security education and decision making at the user level will help prevent your organisation being the next victim.

Contact Infosec Partners today for more information on the 'Phishing Exposure Assessment' and other security testing and managed security services designed to protect your organisation and manage risk.

Executives targeted more than ever

Company executives and additional high-level employees are targeted by personalized spear phishing attacks.

Whaling - attacks on the big fish in a company - has seen a dramatic rise but instead of aiming to get the CEOs etc. to disclose information, the identities of the executives are also being assumed to scam other employees within the organisation, using emails containing their specific names, job titles, phone numbers, and more within the email body.

Business Email Compromise (BEC) has yielded $2.3 Billion USD since October 2013 to cyber criminals, according to the FBI.

InfosecPartners
CYBERSECURITY

A trusted advisor to significant organisations, Infosec Partners provides full-spectrum information security expertise and managed services to some of the world's largest and most sensitive businesses, high-profile individuals and families.

www.infosecpartners.com

Speak with a trusted advisor today:

+44 845 257 5903

secure@infosecpartners.com