CYBERSECURITY

365 ARCHITECHS

Information Sheet
Phishing Attacks

Tags: Cybersecurity, Attack Vectors, Cyber Threats

Phishing is an illegitimate attempt to obtain information by way of deception in an electronic communication. Almost one third of all breaches in the past year involved some form of phishing. Organisations should ensure they take positive steps to reduce their cyber risks associated with phishing attacks.

Phishing is part of a collection of social engineering attack vectors, whereby a person is influenced to take an action which may not be in their best interest.

Types of Phishing

Phishing	Spear Phishing	Whaling	Vishing & SMiShing

Phishing attacks are typically emails, where threat actors spoof their email address so that it looks like the sender is someone legitimate. Their intention is usually to trick someone into providing information such as a password or personal details or enticing them to click on a link or attachment to deploy malware.

Spearphishing is a phishing attack aimed at a specific individual. This might follow some ordinary phishing attacks where general information about the individual was divulged. The more tailored, relevant and comprehensive the information available to a threat actor, the more likely they will be able to deceive a victim.

Whaling is a form of Spearphishing aimed at the very big fish such as directors and C-level executives. It can be more difficult to fool a high-value target, but the payoff can be much higher.

Vishing, or voice phishing, phone scams or telephone fraud operates the same way as an email phishing attack, except that the process is done via a phone call rather than an email. Phone numbers may be spoofed to add authenticity to an attack. Threat actors may pose as an authority figure, such as a manager to attempt to elicit information.

SMiShing is similar to vishing, except that mobile phone text messages are used to coerce an individual into downloading malware, visiting a malicious website or calling a fraudulent phone number.

Defences against Phishing Attacks

Security Awareness Training	Procedures	ATP	SPF DKIM DMARC

Often the best defence against phishing attacks is **security awareness training** for users. However, threat actors continually improve the quality of their attacks, making them increasingly difficult to identify. **Simulated attacks** that lead to educational information can be used as part of a training program.

Reviewing **procedures**, particularly regarding financial transactions may identify opportunities to implement separation of duty controls to manage phishing attack risks.

Implementing an **advanced threat protection** (ATP) solution that incorporates zero-day detection of suspicious links and attachments may also assist.

A combination of email system tools known as **Sender Policy Framework** (SPF), **DomainKeys Identified Mail** (DKIM) and **Domain-based Message Authentication, Reporting and Conformance** (DMARC) offer additional protection against spoofed email addresses. This technology can also assist in reducing email spam.

About us
365 Architechs is a technology company based in Brisbane, Australia. We deliver solutions to support organisations on their digital transformation including cloud, modern applications, cybersecurity and artificial intelligence to drive profitability, growth and achievement of strategic objectives.
(07) 3393 1186 | www.365a.com.au | sales@365a.com.au

Disclaimer
These Information Sheets are designed to provide general information only. They should not be relied upon without consulting professional advice on your specific circumstances. 365 Architechs will not be held liable for any acts or reliance upon the information provided contained within.