Requirements and Testing Procedures		Guidance
5.4 Anti-phishing mechanisms protect users against phishing attacks.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Technical controls can limit the number of occasions personnel have to evaluate the veracity of a communication and can also limit the effects of individual responses to phishing. **Good Practice** When developing anti-phishing controls, entities are encouraged to consider a combination of approaches. For example, using anti-spoofing controls such as Domain-based Message Authentication, Reporting & Conformance (DMARC), Sender Policy Framework (SPF), and Domain Keys Identified Mail (DKIM) will help stop phishers from spoofing the entity's domain and impersonating personnel. The deployment of technologies for blocking phishing emails and malware before they reach personnel, such as link scrubbers and server-side anti-malware, can reduce incidents and decrease the time required by personnel to check and report phishing attacks. Additionally, training personnel to recognize and report phishing emails can allow similar emails to be identified and permit them to be removed before being opened. It is recommended (but not required) that anti-phishing controls are applied across an entity's entire organization. *(continued on next page)*
5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	**5.4.1** Observe implemented processes and examine mechanisms to verify controls are in place to detect and protect personnel against phishing attacks.	
Customized Approach Objective		
Mechanisms are in place to protect against and mitigate risk posed by phishing attacks.		
Applicability Notes		
This requirement applies to the automated mechanism. It is not intended that the systems and services providing such automated mechanisms (such as email servers) are brought into scope for PCI DSS. The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		