Guidelines for C-suite Employees of an Organisation

No	Guideline	Rationale
G26	*Follow a consistent template for organizational emails and create a standard template for anti-phishing webpages.*	• A consistent email structure helps employees to notice the discrepancies in phishing emails easily [P41]. • A standardized template for anti-phishing webpages reduces inconsistency helps avoid confusion and helps web-designer implement their anti-phishing tools easily [P42].
G27	*Introduce a user-friendly, built-in phishing reporting tool within the client system. Develop a formal procedure to handle phishing reports.*	• Having a formal procedure placed makes it convenient to handle phishing reports [P50]. • An in-client phishing incident reporting tool makes phishing reporting easier [P58, P63].
G30	*Create a structured policy and documentation. Regularly assess and manage phishing awareness efforts.*	• Appropriate policy and documentation ensure that all the employees adapt themselves to security countermeasures and requirements [P26, P38, P60]. • Continuous measurement, improved management and policy making helps to achieve improved phishing defence [P11, P38, P40, P50, P53, P54, P57, P67].
G39	*Train users how to report phishing and reward secure behaviour.*	• Training users on how to report phishing incidents and explaining the benefits of reporting can help to establish a phishing reporting culture [P26, P50, P58, P60, P69]. • Rewarding employees for their secure behaviour can motivate and encourage them to perform better [P30, P61, P66].