Guidelines for Information Security Team of an Organisation

No	Guideline	Rationale
G12	*Offer intervention immediately after users fall for phishing.*	• Avoiding delay in displaying warnings minimizes users' confusion [P5]. The right timing of training intervention provides instant education [P2].
G15	*Use both technical and human-centric defence mechanisms to cope with phishing.*	• Prevent user's over-reliance on technology, provide additional defence in detecting unpredictable, highly dynamic, and increasingly sophisticated phishing attacks [P3, P5, P12, P17, P18, P26, P27, P28, P38, P41, P51, P53, P57, P58, P59]. • Educating users about the security properties of different interventions remove their misunderstanding that leads to mistake [P14]. • Training all individual who has access to the organization increase the organization's robustness [P53]. • Human-centric defence mechanisms organized by C-suit employees can help low-level employees in the organization to learn about phishing [P21, P38, P40, P56, P57, P59, P61, P67, P68, P69].
G16	*Personalize the intervention style and medium based on the target user's demographic.*	• Personalized phishing training can take into account user's preferences (e.g., individual preferred training method [P15, P21], content relevant to the organization [P16, P58], roles and responsibilities [P40, P53, P58, P60], age [P21, P35]) to ensure users receive targeted education and training [P7, P13, P15, P16, P21, P26, P35, P36, P40, P48, P52, P53, P57, P58, P59, P60, P61, P62, P64, P66, P67]
G18	*Configure IT system for phishing training.*	• Preparing IT system to avoid simulated email being filtered by technical filters helps users being missed for training [P69]. • Verifying if inventory management software is utilizing scanning, analysis, or probing techniques help detect abnormally high levels of external IP addresses [P54].
G20	*Use automated platforms and improved tools for phishing training, incident management and reporting.*	• Automated approaches help to better support managing complex situations, delivering personalized content and threat identification [P61, P63, P67, P50].
G24	*Send pre-notification to the users before conducting phishing training, however, perform random phishing training.*	• Sending pre-notification to the participants prevents discomfort [P30, P69].

		• Emphasising on the anonymity of phishing training can reduce the effect of prairie dogging and estimate of organization's likelihood to fall victim to phishing [P59, P61, P62, P69]
G25	*Conduct prior investigation before adopting anti-phishing tools, identify most vulnerable group and determine priority topics.*	• Perform prior research and analyze the reviews on tool vendors to select the right tool [P26, P61] • Identifying vulnerable users can help reduce training time and efforts [P26]. • Teaching everything or huge amount of information can cause security fatigue [P13].
G28	*Get employees' feedback to modify the organization's policy.*	• Obtain staff's feedback after phishing simulation to modify the organization policy accordingly to meet staff's needs [P50].
G29	*Deploy help-desk and victim support for users.*	• Deploying post simulation help desk support allows further users' investigations [P51]. • Deploying help-desk support can assist external users in determining the authenticity of an email sent from the organization [P51]. • Add a victim support option in the anti-phishing webpages can help users to fix potential problems [P42].
G31	*Conduct phishing simulation with embedded training.*	• Assist the organization's security team in practicing the handling and response to simulated phishing incidents to enhance preparedness for real phishing attacks [P53, P56, P57, P60, P61]. • Embedding learning content with phishing simulation provides education on demand [P5, P7, P12, P27, P53, P56, P57, P58, P59, P60, P61, P67, P68, P69].
G32	*Conduct phishing simulation that adheres to the guidelines of the data privacy policy appropriate to the region.*	• Data privacy policy-compliant phishing training protects participants sensitive information, hence reducing data breaches [P26, P69].
G33	*Provide users immediate feedback on their performance.*	• Users feel motivated if instant corrective feedback is provided after testing and evaluating their phishing knowledge in their regular environment [P7, P10, P31].
G34	*Use realistic and equally difficult training emails. Use challenging questions to test phishing knowledge.*	• Realistic and equally difficult email helps to test the persistence of the training's effect [P7]. • An extensive test with challenging questions reduce repetitive training costs and can help avoid the ceiling effect [P21].
G35	*Implement progressive and self-adaptive phishing training.*	• Dynamic and self-adaptive phishing training improve user sensitivity to deception cues [P24, P63, P64, P66].

G36	*Adopt video and interactive education and training materials.*	• Video and interactive training are more effective as users do not need refreshment very quickly [P5, P11, P19, P34, P36]
G37	*Utilize the expertise of external service providers to aid in phishing knowledge assessment and awareness material development.*	• Leveraging external service providers can support better phishing knowledge assessment and awareness material development [P54, P60].
G38	*Choose evaluation metrics and baselines that are useful and relevant.*	• Click-through rate should be normalized based on the persuasiveness of the training template to produce a sound analysis and evaluation [P32, P54, P56, P58, P59, P60, P61, P68].
G40	*Conduct multiple cycles of follow-up training.*	• Help to assess users' short-term and long-term knowledge retention after training [P26, P31, P52, P54, P57, P58]. • Repetitive training in a short period helps users learn a second time if they had difficulty understanding in the first time [P5, P7, P24, P27, P34, P53, P56, P57, P62, P67, P68, P69]. • Follow-up training (for children) to counter knowledge decay of the ability to identify phishing [P21].
G41	*Avoid frequent reminders and over-training and keep the reminders short and simple.*	• Avoiding frequent risk notifications and over-training reminders can reduce training fatigue [P34, P52, P53, P58, P60, P61, P62, P69]. • Including a lower bound of information in the reminder measures can reduce security fatigue [P34].