TABLE I: Guidelines for anti-phishing interventions

No	Guidelines	Rationale
G1	Remove deceptive user interface elements for unverified emails and incorporate an alert icon within the email client to indicate potentially fraudulent emails.	• Disabling misleading UI elements (e.g., profile photo, email history) for unverified sender addresses will reduce user confusion [P16]. • Placing a security indicator for unverified email delivered to the user acts as a forcing function for the sender domain to configure their SPF/DMRC/DKIM correctly [P7, P16].
G2	Clearly display the underlying URL of a suspicious link in the email client	• Clearly displaying the underlying URL of a suspicious link in the email client (link-focused warning) make it easier for users to notice where the links' actual destination [P25].
G3	Incorporate progressive disclosure in the design and add a learn more button.	• Progressive design and learn more buttons help to facilitate general advice, satisfy user curiosity, and support user investigations [P4, P5, P25, P51].
G4	Use visual examples and explanations and avoid technical jargon in the content.	• Avoiding technical details in the content can make them understandable to non-expert users [P1]. • Integrating visual examples and explanations on phishing cues presented helps users memorize and understand better [P42].
G5	Present abstract information and leverage situated learning in the content.	• Leveraging situated learning in the design can make the intervention interesting and engaging, and also improves learning outcomes [P5, P10, P19, P28, P34, P36, P37, P61, P62]. • Too much information in the content can be unappealing to inexperienced users [P1, P5, P13, P18, P41]. • Adopting situated learning is beneficial as learning science suggest that simply asking users to follow some advice would not be helpful [P5].
G6	Introduce varieties in the content and keep the information up to date.	• Including varieties in the content can help users tackle new and emerging phishing attacks [P19, P57, P58, P59, P61, P65].
G7	Minimize the functions and frequency of intervention users need to encounter.	• Limiting the frequency of the warnings reduce warning fatigue [P4]. • Minimum number of functionalities in the game can help finish the game easily, easy for users to remember when functionalities are less [P10].
G8	Design phishing warnings differently from standard warnings.	• Variation in the design increases the likelihood for users to read it, ensures they are taken seriously and prevent habituation [P1, P2, P14].
G9	Make the critical information easily accessible and visible to the users.	• To make users easily notice the warnings [P1, P4, P8, P25], increase warning adherence [P25] and to impose forced attention [P8, P25].
G10	Create uniform phishing indicators across different browsers and mobile interfaces.	• This will reduce the susceptibility of mobile device users [P16].
G11	Provide users clear choices and actionable items to proceed.	• Active interruption and actionable items minimize the user's workload, are naturally noticeable and users can use their time efficiently [P1, P2, P4, P5, P7, P20, P22, P24, P25 P41, P43, P44]
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].
G13	Perform usability tests and collect user feedback.	• Collecting users' feedback from usability testing can improve future intervention design [P18, P22, P57, P61, P66, P67].
G14	Provide an explanation to the users on anti-phishing system reliability and decision-making and clarify users about the objective of the intervention.	• Feedback on the anti-phishing system increases users' trust [P7, P8, P11, P14, P33, P39, P43], helps users perceive potential danger [P20], increases user understanding and improves user ability to detect phishing [P18, P39]. • Making it clear to the users why they have displayed the intervention or not taken to the website to avoid their confusion [P5,P14].
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].
G17	Consider the decision-making process and vulnerabilities of humans in the design.	• Taking into account the vulnerabilities and decision-making processes of the user (e.g., users' misconceptions and perspectives [P11], perceived threat [P9]) increases the effectiveness of anti-phishing interventions for end users and assist to develop the tailored approach [P4, P6, P7, P9, P11, P18, P24].
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].
G19	Design visually distinct user-friendly URL bar.	• Noticeable and consistent URL bar helps users differentiate legitimate and malicious domains easily [P2, P8, P46].
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].

Continued on next page

Guidelines for anti-phishing interventions – continued from previous page

No	Guidelines	Rationale
G21	Disable JavaScript on login forms when a form element is in focus.	• Deactivating JavaScript on webpages every time the focus is put on a form element prevents the attacker from capturing the keystrokes or initiating timing attacks [P16, P22, P23].
G22	Explain the capabilities and effectiveness of the deployed anti-phishing solution clearly to the users.	• Reliable trust signals to the users can prevent over-trust and over-reliance on the deployed anti-phishing solutions [P11]. • Utilizing interactive error messages to elucidate the purpose of a website can deter users from engaging in destructive actions [P43, P44].
G23	Use email authentication protocols to encrypt emails and filter out incoming malicious emails.	• To achieve better resiliency [P18,P51] and to make more informed decision [P16, P27] on the incoming emails.
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].
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].
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].
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].
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].
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].
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].