Guidelines for Designer/Developers

No	Guideline	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]
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].
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]
G19	*Design visually distinct user-friendly URL bar.*	• Noticeable and consistent URL bar helps users differentiate legitimate and malicious domains easily [P2, P8, P46].
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.
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].