TABLE I: Critical success factors in PETA [Symbols E, T and A refer to critical success factors related to education, training, and awareness respectively]

Critical success factors	Key points (included papers)	#
Design		
CSF1. Design of engaging and up-to-date training content [E] [T]	• Incorporating situated learning to improve user engagement [P5,P10,P19,P28,P34,P36,P37,P61,P62] → Ch2.❶ • Including up-to-date content in the phishing training [P57,P59] → Ch2.❸	11
CSF2. Design of comprehensible anti-phishing technology [E] [A]	• Detailed report on anti-phishing efforts to persuade users to adhere to the warning and to support non-expert users [P33,P45] → Ch4.❹ • Explicit anti-phishing protection tools to increase users trust on automated anti-phishing tools [P11,P39] → Ch5.❷ • Integrate both visual and text example with explainability in the anti-phishing webpages [P42] • Designing user friendly URL bar to remove users domain name confusion [P8] → Ch11.❶,Ch.11❷ • Providing users with reliable automated anti-phishing tools [P7,P8,P14,P33] → Ch5.❷	8
CSF3. Diversity in training content to educate users on evolving phishing attack [T]	• Use of variety of training content, mix of tools for phishing training [P58] → Ch2.❸ • Attack vector variation in the phishing training content [P19,P61,P65] → Ch2.❺	4
CSF4. Consistency in the design [E] [A]	• Creating a standard unified template for anti-phishing webpages [P42] • Organizations should practice using the same structure and features for legitimate emails [P41] • Legitimate domain should avoid using common domain squatting techniques [P46]	3
CSF5. Design of tailored phishing intervention [E] [T] [A]	• Customised phishing training design for employees with power and authority in organization [P40] • Prioritising topics for training relevant to the organization [P16,P58] • Taking account the target demographic into training design and execution [P48] • Personalized training content [P26,P52,P53,P57,P59,P62,P66,P67] → Ch7.❶ • Considering casual and serious gamers need in the game design [P36] • Dynamic and self-adaptive phishing training [P63,P64,P66] • Personalized communication style and medium for phishing training [P61,P62] • Text training materials instead of comic materials in corporate settings [P7] • Developing anti-phishing tools for children [P21,P35] → Ch16.❶ • Web application dressing according to user preferences [P49]	21
CSF6. Improving the UI design [E] [A]	• Disabling misleading UI elements for unverified emails [P16] → Ch1.❷ • Design of consistent phishing indicators for different interfaces [P16] → Ch1.❶ • Use of various colours [P5,P7] • Avoid using the same personalized indicators across different interfaces [P31] • Adding a support button in the email client to support user investigations [P51] • Adding an icon in email client indicating suspicious email [P7] → Ch1.❸ • Limiting the number of warnings user encounters to reduce warning fatigue [P4] → Ch3.❷	6
CSF7. Design of informative and concise warning [E] [A]	• Present abstract information using concrete examples [P1,P5,P13,P18,P41] → Ch4.❷ • Incorporate progressive disclosure in the design [P4,P5,P25] → Ch2.❸ • Warning should provide clear choice to the user [P1,P2,P5,P14]	9
CSF8. Incorporating users' psychological and behavioral aspect in the design [T] [A]	• Considering human vulnerabilities and decision making process in the design [P9,P11,P18,P24] → Ch8.❶,Ch8.❷,Ch8.❸ • Perform usability testing to improve warning design [P22,P57,P61,P66,P67] → Ch5.❶	9
CSF9. Integrating phishing simulation with embedded training to facilitate education on demand [T]	• Supplementing the phishing simulation with learning content [P5,P7,P12,P27,P53,P57,P58,P59,P67,P68,P69]	11
CSF10. Focus on active warning designs [A]	• Visual aids for safe browsing to draw user attention [P8] • Link focused warning in the email client to grab user attention [P25] • Warnings need to be actively interrupting users' primary tasks [P1,P2,P20,P22] → Ch3.❹ • Design of phishing warnings should be different than trivial warnings [P1,P14] → Ch3.❶ • Phishing indicators should distort the visual appearance of the website to help users distrust the phishing website [P1] • Warnings should stay long enough to grab users' attention [P1] • Action based inhibitor in the warning to reduce users cognitive burden and potential hazard of clicking malicious links [P22,P25] • Use of forcing and negative training functions [P43,P44]	9
Implementation		
CSF11. Bringing key stakeholders on board to educate and encourage employees [T] [A]	• Important role should be played by the C-suite to secure the organization against phishing [P38,P40,P56,P57,P59,P61,P67,P68,P69] • Universities and practitioners should come forward to educate people [P21] • Leverage external service providers to support on phishing knowledge assessment and awareness material development [P54,P60]	12

Continued on next page

Critical success factors in PETA – continued from previous page

Critical success factors	Key points (included papers)	#
CSF12. Strengthen authentication and encryption mechanisms in browsers and email clients A	• Use single domain name and use SSL to encrypt websites [P2] → Ch14.❶ • Deploying browser based authentication [P8] • Adoption of SMTP security extensions in email applications [P16] → Ch14.❷ • Deactivate or re-activate javascript to avoid keystroke or timing attack [P16,P22] → Ch13.❶, Ch13.❷	4
CSF13. Feedback, reminders and reinforcement to maintain phishing awareness among users T	• Avoid frequent risk notification, avoid regular reminders, provide feedback to help maintain awareness [P53,P58,P60,P61,P62,P69] • Rewarding secure behavior [P30,P61,P66]	8
CSF14. Conduct GDPR compliant and anonymous training to protect user privacy and avoid false training outcome estimation T	• Conduct GDPR compliant phishing simulation [P26,P69] • Emphasizing the anonymity and learning aspect of the phishing simulation [P59,P69] → Ch17.❸ • Conduct random phishing simulation to reduce the effect of prairie dogging and estimate of organization's likelihood to fall victim to phishing [P61,P62] → Ch17.❸,Ch19.❷	5
CSF15. Providing phishing education and training to critical demographic group E T	• Raise retailers awareness about phishing along with their customers [P64] • Topics on anti-phishing training should be taught in the school to educate children [P21,P35] → Ch16.❶ • Everyone who has influence in organization's security should be trained [P53,P58,P60] • More focus on unmotivated and careless users [P40] • Teacher should be given priorities in terms of phishing education [P21,P35] → Ch16.❶ • Focus on vulnerable group for phishing education [P13]	8
CSF16. Automating the phishing training to support organization's security teams T	• Automation in delivering personalized contents and automation in threat identification [P61] → Ch12.❷ • Automating phishing reporting and incident response processes with the use of improved tools [P50,P63,P67] → Ch12.❶	4
CSF17. Better planning, policy management, and documentation on phishing training E T	• Improved phishing defence through improved management and policy making [P11,P38,P40,P50,P53,P54,P57,P67] → Ch15.❺ • Structured and explainable policy and documentation of phishing training program [P26,P60] • Sending pre-notification to the participants to prevent discomfort [P30,P69] • Perform prior research and analyse the reviews on tools vendors [P61] → Ch15.❷ • Preparing IT system to avoid simulated email being filtered by technical filters [P69] → Ch9.❷ • Deploying post simulation help desk support to support users investigations [P51]	14
CSF18. Enabling and encouraging individuals to report phishing E T	• Establishing phishing reporting culture [P26,P50,P69] • Implementing easy-to-use, in-client phishing incident reporting tool [P58,P63] • Training users how to report phishing incident and explaining the benefits of reporting [P58,P60]	6
CSF19. Invest in both technical and socio-organizational functions and capabilities E T A	• Effective phishing detection requires the combination of technological innovation and human intervention [P3,P5,P12,P17,P26,P27,P28,P38,P41,P51,P53,P57,P58,P59] • Combining strengths of multiple anti-phishing technologies [P18,P51]	15
Evaluation		
CSF20. Conduct intermittent short time progressive training to re-inforce users' phishing awareness T	• Avoid over-training to reduce training fatigue [P52] • Multiple cycles of training to re-inforce phishing awareness [P24,P53,P56,P57,P68,P69] → Ch20.❶ • Repetitive training in a short time span [P5,P7,P27,P34,P62,P67,P69] → Ch20.❶ • Testing users' short-term and long-term knowledge retention after training [P52] → Ch20.❷ • Progressive training [P24]	13
CSF21. Perform empirical testing and statistical analysis to improve and better support phishing training T	• An extensive test with challenging question to reduce repetitive training cost and avoid ceiling effect [P21] • Conducting phishing simulation [P56,P57,P60,P61] • Assessment of long term impact [P31,P54,P57,P58] • Selection of effective metrics and relevant baselines [P54,P56,P58,P59,P60,P61,P68]	10
CSF22. Investigate if the phishing simulation is affected by false positives to avoid erroneous evaluation T	• Check if inventory management softwares are using any scanning, analysis or probing to identify unusually high volume of external IP addresses [P54] → Ch19.❶ • Normalize and re-scale click though rates for more accurate assessment [P32]	2
CSF23. Conduct user evaluation in their regular environment with realistic emails and measure delayed outcome to replicate real world settings E T A	• Preserve users actual behavior to achieve results close to real world settings [P2,P18,P43] → Ch16.❸ • Use of field techniques for high ecological validity [P4] → Ch16.❸ • Testing users in their normal environment with instant corrective performance feedback [P7,P31] → Ch16.❸ • Realistic and equally difficult training emails to test the persistence of training outcome [P7] • Use of real-time brain-eye measure to collect transparent data [P17] → Ch17.❸	7