TABLE I: Challenges in PETA [Symbols E, T and A refer to challenges related to education, training, and awareness respectively]

| Challenges | Key points (included papers) | # |
|---|---|---|
| | **Design** | |
| Ch1. UI design restrictions in the browser and email client<br>A | ① Inconsistent UI design in web browser across different devices creating confusion to users [P22, P49]<br>② Misleading UI design of third party email clients [P16]<br>③ Absence of phishing indicators in third party email and mobile client [P16] | 3 |
| Ch2. Content restrictions for phishing education and training<br>E T | ① Lack of engaging and interesting phishing education and training material [P10,P19,P28]<br>② Presence of complex interface and configuration in the game design [P28]<br>③ Repetitive training content [P7]<br>④ Disregard for user misunderstandings and interests [P11,P19]<br>⑤ Limited attack vector consideration [P19,P24,P59]<br>⑥ Disregard for both casual and serious gamers [P36]<br>⑦ Presence of cultural bias in the content [P36]<br>⑧ Time consuming decision making process and lengthy training email [P5,P7] | 9 |
| Ch3. Design constraints for anti-phishing warning UI interfaces<br>A | ① Design similarity of phishing warnings with less serious security warnings [P1,P28]<br>② Frequent exposure causes warning fatigue [P4,P13,P14,P17,P18,P26]<br>③ Unsuitable warning placement [P2,P3,P5,P7,P11,P15,P25]<br>④ Absence of active user interruption [P1,P11,P14,P43,P44] | 17 |
| Ch4. Problems with Anti-Phishing warning content<br>A | ① Lack of comprehension and explainability [P14,P25,P49]<br>② Lengthy content [P41]<br>③ Distinct phishing warning design among vendors, platforms and web version [P49] | 5 |
| Ch5. Performance limitations of anti-phishing tools<br>A | ① Inadequate usability [P1,P2,P8]<br>② False positives and lack of reliability [P1,P2,P3,P8,P10,P13,P14,P18,P24,P25,P28,P44,P49,P57,P69] | 15 |
| Ch6. Lack of attention to phishing indicators<br>E T A | ① Ignorance due to lack of trust and understanding on phishing warning and training [P1,P2,P3,P4,P8,P11,P14,P24,P28,P31,P36,P39,P44,P49]<br>② Disregard to warning due to appealing web content and site reputation [P2,P8,P14,P24,P49] | 14 |
| Ch7. Need to design specific training for spear phishing<br>T | ① Difficulty to detect spear phishing due to personal relevance and familiarity [P1,P7,P14,P15,P21,P26,P49,P58] | 8 |
| Ch8. Disregard for users' mental limitations during design<br>E T A | ① Users' distraction by other tasks is not well considered [P2,P7,P8,P13,P14,P24,P47]<br>② Users' inattentiveness to phishing interventions have not been taken into account [P7,P13,P14,P17,P24,P58]<br>③ Current design practices unconditionally rely on user decision [P4,P15,P17,P24,P25,P40,P49]<br>④ No alternative options for users to help them complete their primary task [P2] | 14 |
| | **Implementation** | |
| Ch9. Anti-phishing technology deployment challenge<br>E T A | ① Deployment difficulty of anti-phishing technologies due to interdependancy on multiple factors and platform dependency [P23,P38,P50]<br>② Complicacy to safeguard employees in distributed and siloed settings due to enlarged attack surface [P6,P54,P57,P62,P65]<br>③ Training email spammed by email provider [P28] | 9 |
| Ch10. Technology adoption and usage challenges<br>E T A | ① Requirement of prior experience and investment in software for phishing games [P37,P45]<br>② Requirement of expertise and assistance from third-party services [P1,P8,P45]<br>③ Requirement of users' effort and willingness to use anti-phishing warnings [P19,P31,P45] | 6 |
| Ch11. Challenges due to complicated URL and domain name structures<br>E T | ① Similar organization name in the URL [P2,P45]<br>② Difficulties to detect minor changes in URLs [P46]<br>③ User confusion to identify phishing website hosted by trustworthy websites [P45]<br>④ Presence of textual manipulations and complex visual tricks in the URL [P45,P47] | 4 |
| Ch12. Obstacles to automate phishing incident response and anti-phishing training<br>E T A | ① Handling phishing incident reports requires the need for human validation [P50]<br>② Embedded training deployment requires manual human effort [P45] | 2 |
| Ch13. Exploitation of software vulnerabilities by attackers<br>A | ① Use of malicious javascript codes by attackers to bypass monitoring phishing plugins [P23]<br>② Use of XSS by the attackers to inject malicious code into legitimate webpages [P49] | 2 |
| Ch14.Unguarded email clients and websites<br>A | ① Limited use of SSL indicator to protect website login page [P2]<br>② No built in mechanism in SMTP to prevent phishing [P16] | 2 |

Continued on next page

Challenges in PETA – continued from previous page

| Challenges | Key points (included papers) | # |
|---|---|---|
| Ch15. Limitations of current anti-phishing planning, policies and guidelines<br>E T A | ① Contradicting, incomplete and outdated anti-phishing recommendations in organizational websites [P15,P42]<br>② Choice of customized or outdated tools to manage IT incidents impact service quality and efficiency [P50]<br>③ Poor practice of training execution [P12,P59]<br>④ Lack of formal approach to gain experience from previous phishing incidents [P50]<br>⑤ Inadequate policies and guidelines to invoke user behavioral change [P50] | 5 |
| **Evaluation** | | |
| Ch16. Lack of industrial relevance in evaluation practices and settings<br>E T A | ① The neglect of young people to test and improve their phishing knowledge [P21,P35]<br>② Sample bias due to limited demographic consideration [P1,P13,P14,P30]<br>③ Failure to conduct usability testing in real-world settings [P1,P7,P26]<br>④ Poor evaluation practices results in unreliable outcome [P14,P18,P32] | 10 |
| Ch17. Complications regarding data collection and replicating user experience<br>E T A | ① Difficulty to emulate users real-life experience in phishing studies [P3,P43,P31]<br>② Ethical difficulties of conducting phishing studies [P48]<br>③ Challenges of phishing study due to bias induced by the participants [P14,P21,P40] | 7 |
| Ch18. Insufficient usability and effectiveness evaluation of phishing interventions<br>E T A | ① Negligible practical value and effectiveness evaluation [P4,P8,P13,P18,P37,P40]<br>② Inadequate empirical investigation on variables used in phishing training and detection [P30,P41]<br>③ Lack of understanding on user behavioral response towards phishing incidents [P17,P33,P41] | 10 |
| Ch19. Lack of sophisticated quantification of phishing training outcome<br>T | ① Difficulty in measuring user phishing training effectiveness due to presence of bots [P55]<br>② Impact of pairie dogging on phishing training program outcome [P15,P59] | 3 |
| Ch20. Lack of post-training user knowledge retention practice<br>E T | ① Effectiveness of phishing interventions subject to dwindle over time [P13,P21,P40,P45]<br>② Lack of investigation on users' long term behavior change [P7,P31,P34,P54] | 8 |