Table 1. List of identified challenges from the multi-vocal literature review:

|  |  |
| --- | --- |
| **No.** | **Challenges** |
| **Design challenges** | |
| Ch1. | UI design restrictions in the browser and email client |
| Ch2. | Content restrictions for phishing education and training |
| Ch3. | Design constraints for anti-phishing warning UI interfaces |
| Ch4. | Problems with anti-phishing warning content |
| Ch5. | Performance limitations of anti-phishing tools |
| Ch6. | Lack of attention to phishing indicators |
| Ch7. | Need to design specific training for spear phishing |
| Ch8. | Disregard for users’ mental limitations during design |
| **Implementation challenges** | |
| Ch9. | Anti-phishing technology deployment challenge |
| Ch10. | Technology adoption and usage challenges |
| Ch11. | Challenges due to complicated URL and domain name structures |
| Ch12. | Obstacles to automate phishing incident response and anti-phishing training |
| Ch13 | Exploitation of software vulnerabilities by attackers |
| Ch14. | Unguarded email clients and websites |
| Ch15. | Limitations of current anti-phishing planning, policies, and guidelines |
| **Evaluation challenges** | |
| Ch16. | Lack of industrial relevance in evaluation practices and settings |
| Ch17. | Complications regarding data collection and replicating user experience |
| Ch18. | Insufficient usability and effectiveness evaluation of phishing interventions |
| Ch19. | Lack of sophisticated quantification of phishing training outcome |
| Ch20. | Lack of post-training user knowledge retention practice |