TABLE I: Individual, Technical and Organisational Factors and Their Impact on Anti-phishing Interventions

No	Factors	Impact	No of studies
		Individual human factors	
D1	Age	• Children aged 8-13 require specialized phishing educational intervention as they are biologically less attentive [P21, P35]. • Teenagers tend to make decisions quickly without considering the consequences, and are more susceptible to being persuaded by urgency and panic-inducing phishing emails [P35]. • Older employees have relatively bad training outcomes as they prioritize maintenance over growth [P40]. • Age 18-25 are vulnerable to phishing attacks [P6].	4
D2	Complacency	• Users' overconfidence in the appealing web content leads them to disregard phishing warnings [P2, P5, P8, P11, P49]. • Users' prior experience with websites results in overconfidence, causing them to disregard phishing warnings [P1, P2, P5, P11, P13, P25, P44]. • Users over-rely on site reputation and trust the warning [P14]. • Users are overconfident about their ability to detect phishing [P43, P44, P45], over-trust on their organizational technical phishing solutions [P7].	14
D3	Confusion	• User confusion arises due to similarity in domain names [P45], webhosting [P45, P49], distinct warning design patterns among vendors [P25, P49] and conflicting information present in the anti-phishing guidelines [P42]. • Users become confused about the purpose of a received training email [P5].	5
D4	Curiosity	• Users click on the phishing link out of curiosity [P2, P25].	2
D5	Distraction	• Users are distracted by other tasks as security is not their main concern [P13, P14, P41]. • Individuals are unable to focus on multiple things simultaneously (e.g., noticing on phishing warning while doing online shopping) [P13].	3
D6	Educational Qualification	• Phishing stories from a peer is an effective method of training for college students [P48]. • University staffs learn better from facts from an expert-based training method [P48]. • Compared to bachelor's degree, users having master's and PhD degrees are more confident in detecting phishing [P52].	2
D7	Knowledge decay	• The knowledge gained by users during phishing training tends to dissipate over time [P7, P13, P21, P31, P34].	5
D8	Ignorance	• Users failed to look at anti-phishing interventions [P7, P13, P17, P28], ignored as web content looked legitimate [P2] and when received a high frequency of warnings [P4].	6
D9	Lack of communication	• Before designing and implementing anti-phishing software, users' interests and needs are not well investigated [P16].	1
D10	Lack of motivation	• Users are not motivated enough to install anti-phishing software on their devices [P31, P37], show unwillingness to report phishing due to a complicated reporting process [P50, P58, P63] and do not find the training and educational material interesting [P10, P19, P28].	8
D11	Lack of trust	• Users do not trust anti-phishing warnings due to limited accuracy of anti-phishing tools [P1, P11].	2
D12	Optimism bias	• Optimistic users tend to be less conscious as they believe that negative events only happen to others [P13].	1
D13	Perceived vulnerability and severity	• An individual's heightened understanding of the consequences of phishing attacks enhances their resistance to these types of attacks [P40].	1
D14	Pressure	• Phishing incident response by IT staff gets delayed due to the reception of a high volume of phishing reports [P50]. • An individual receiving a high volume of emails is more susceptible to phishing attacks [P26].	2
D15	Fatigue	• Providing comprehensive instruction could result in overwhelming the user [P13]. • Frequent exposure to warning causes warning fatigue [P4, P13, P14, P17, P18, P26]. • Frequent risk notifications and excessive training result in training fatigue [P34, P53, P58, P60, P61, P62, P69].	13
		Technical factors	
D16	Device type	• Individuals who rely on mobile devices are at a higher risk, as phishing signs are obscured or not fully visible on the small screens of mobile devices [P49].	1
D17	Gamer type	• A casual player is unsatisfied with playing a phishing game that is designed for serious gamers, and conversely, a serious gamer is unfulfilled playing a phishing game that is intended for casual players [P36].	1
D18	Lack of knowledge	• Users do not understand anti-phishing warnings due to lack of knowledge about security and security indicators [P1, P4, P5, P6, P7, P8, P9, P10, P11, P13, P14, P17, P20, P21, P28, P35, P39, P46, P47, P49].	20
D19	Lack of resource	• User do not have enough infrastructure support when they work from home [P6]. • Absence of abstractness in the anti-phishing recommendations and lack of advanced anti-phishing tools reduces users' self-efficacy [P42]. • Users do not receive training emails due to emails being in the spam folder [P28].	3
		Organizational factors	
D20	Organizational position	• Employees in a higher position in an organization are more vulnerable regardless of the phishing training or punishment [P40].	1
D21	Social influence	• People trust others' phishing stories as they perceive this information as trustworthy [P15]. • Observing others share information results in heightened levels of disclosure [P13]. • The motivation, self-efficacy, and cognitive ability of employees are impacted by the social relationships within and surrounding the organization [P26, P40].	4
D22	Norms	• Organization's procedural measures (e.g., security policies, standards and guidelines) have a beneficial effect on raising security consciousness [P38].	1