Table 1: Identified intervention types

No	Intervention	Description
		Phishing education
E1	Anti-phishing instruction	Anti-phishing instructions (e.g., anti-phishing webpages [P42], posters or leaflets on how to deal with phishing [P13]) aim to provide guidance to the users about several aspects of phishing attack, for instance, about the best practices to recognise phishing attacks, instructions on how to report phishing attacks.
E2	Educational game	Taking a didactic approach, phishing educational games provide users with information and resources to help them better understand the topic of phishing [P9, P10, P11, P36, P37].
		Phishing training
T1	Phishing simulation and Embedded training	In phishing simulation and embedded training, organisations send simulated phishing emails to their employees from a specialised phishing simulation software or service to test employees' vulnerability to phishing attacks. In most cases, after an employee takes a harmful action (e.g., clicks on a suspicious link, provides sensitive information, etc.), they are presented with training or learning content that explains the consequences of their actions [P5, P7, P12, P26, P27, P32, P38, P40, P53, P55 to P69].
T2	Phishing training game	Phishing training games often adopt a hands-on, experiential approach to train users about phishing [P19, P28].
T3	Narrative based training	In narrative-based training, users are provided information in the form of stories [P15, P48].
T4	Instructor based training	In instructor-based training, users are delivered tutorials on phishing by a security expert (e.g., chief information security manager [P34], a training expert [P21]).
T5	Information and guidance based training	In this form of training, users are explained certain facts about phishing and then they are advised some guidelines on what to do when they encounter phishing attack. Unlike instructor-based training, this type of training can be provided by anyone, for example, a security expert or a peer [P15, P24].
		Phishing awareness
A1	Email client phishing indicator	Email client phishing indicators work by scanning incoming emails and analysing various factors such as sender's email address, email content, link and attachments or the email header to identify potential phishing attempts [P16, P25].
A2	Browser SSL warning	A Browser SSL warning appears when there is a problem with the SSL certificate for a website. It verifies that the website being accessed is legitimate and that the connection between the user's browser and the website is encrypted [P4, P8, P14, P22].
A3	Browser EV certificate Warning	A browser EV (Extended Validation) certificate warning, on the other hand, provides a higher level of security and validation. In addition to verifying the domain, an EV certificate requires additional verification of the organisation or entity behind the website, including legal and operational checks [P8].
A4	Browser security toolbar	Browser security toolbars are add-ons or extensions that can be installed on a web browser to provide additional protection against phishing attacks. These toolbars may include features such as URL scanning, page analysis, real-time updates, and user reporting to help detect and block known phishing websites. Additionally, some browser security toolbars may include other security features, such as blocking pop-ups or disabling scripts, to further protect the user against malicious content [P2, P18].
A5	Browser phishing warning	Browser phishing warnings (active or passive) are built-in security features of web browsers [P1, P4, P14, P17, P23, P25].
A6	QR code scanner phishing warnings	QR code scanner phishing warnings provide anti-phishing warnings to users by checking the links contained within the scanned QR code against a database of known malicious URLs [P20].
A7	Interactive custom phishing indicator	Interactive custom indicators force the user to interact with her customized (personal) indicator (image/text) to log in [P3, P43, P44]