SYSTEMATIC COMPARISON OF ONLINE RISK PERCEPTION LITERATURE (2022-2026): TOWARD A UNIFIED FIVE-DIMENSION FRAMEWORK

AIYUDA, N.[1*] – ISA, K.[1] – JOHAR, S. S. H.[1] – AHDA, M. H.[2]

[1] *Centre for General Studies and Co-Curricular, Universiti Tun Hussein Onn Malaysia (UTHM), Johor Bahru, Malaysia.*

[2] *Department of Communication Science, Universitas Abdurrab, Riau, Indonesia.*

**Corresponding author*
e-mail: gl240013[at]student.uthm.edu.my

(Received 07th August 2026; revised 02nd October 2026; accepted 14th October 2026)

Abstract. Online risk perception has become a key construct in the research on digital behavior. The field is characterized by theoretical heterogeneity and inconsistency in dimensions. This systematic review aims to synthesize the literature published between 2022 and 2026 to address three objectives: (1) to map the theoretical frameworks used to understand online risk perception, (2) to identify dimensions common across research contexts with sufficient empirical support to constitute a unified framework, and (3) to suggest operational definitions for five dimensions that will serve as the conceptual basis for future scale development. A systematic search of Scopus using the keywords of online risk and security resulted in more than 70 sources in the areas of e-commerce, cybersecurity, social media, digital banking, crowdfunding, health, and education. The review maps evidence from 14 studies to five dimensions of perceived online risk, namely privacy, security, financial, fraud, and social, with seven theoretical frameworks. Each of the dimensions is clearly defined and supported by a diverse set of research. Four existing measurement tools cover only some dimensions, highlighting the need for a unified instrument to assess online risk perception.
Keywords: *online risk perception, perceived risk dimensions, privacy risk, security risk, financial risk, fraud risk*

Introduction

The growing embeddedness of digital platforms in everyday economic, social, and health activities has elevated online risk perception to one of the most theoretically consequential and practically urgent constructs in contemporary digital behavior research. Online risk perception refers broadly to an individual's subjective evaluation of the likelihood and severity of harm arising from engagement with online environments (Featherman and Pavlou, 2003; Mitchell, 1999; Slovic, 1987). Its influence extends across e-commerce adoption (Tran and Vu, 2023; Nawi et al., 2021; Yang et al., 2014), social media behavior (Hwang et al., 2025; Kožuh and Čakš, 2025; Arruda Filho et al., 2023), digital banking and payment systems (Siregar et al., 2026; Handoko et al., 2022; Kaur and Sharma, 2022), crowdfunding participation (Dempere et al., 2026), and online education (Pörzse and Kenesei, 2026), making it a construct whose adequate conceptualization and measurement are a prerequisite to progress across multiple research domains simultaneously.

Two interrelated problems constrain the field's ability to produce cumulative knowledge. The first is theoretical fragmentation: multiple frameworks: Perceived Risk Theory (Featherman and Pavlou, 2003; Mitchell, 1999), the psychometric paradigm (Slovic, 1987; Fischhoff et al., 1978), the Technology Acceptance Model (Davis, 1989),

Prospect Theory, the Theory of Planned Behavior (Ajzen, 1991), Information Behavior Theory (Jacobson et al., 2022), and Risk Homeostasis Theory; have each been applied to online risk perception, typically in isolation, without systematic integration. The result is a literature in which the same construct is theorized under different conceptual vocabularies, making cross-study comparison difficult and cumulative theory building tenuous. The second problem is dimensional inconsistency: studies report between three and ten distinct risk dimensions depending on their context, domain, and method (van Schaik et al., 2018; Byrne et al., 2016; Garg and Camp, 2012; Gabriel and Nyshadham, 2008), ranging from four cognitive dimensions in e-commerce to ten psychometric hazard characteristics in social networking. No systematic synthesis has established which dimensions are robust across contexts and which are context-specific artifacts.

These problems have direct measurement consequences. Existing instruments for online risk perception: the Internet Risk Perception Scale (Torres-Hernández et al., 2022), the Online Risk Scale (Kanetsuna et al., 2023), the Cybercrime Risk Perception Questionnaire (Vozmediano et al., 2013), and the Virtual World Risk Perception Scale (Arslankara and Usta, 2018); were each developed within specific theoretical traditions for specific populations, and no single instrument covers all five proposed dimensions within a unified, psychometrically validated measure applicable to general adult internet users. This measurement gap motivates the present systematic review. Its objectives are: (1) to map and compare the theoretical frameworks applied to online risk perception in the 2022–2026 literature; (2) to identify the dimensions that recur consistently across multiple research contexts and theoretical traditions; and (3) to propose five dimensions: Perceived Privacy Risk (PPR), Perceived Security Risk (PSR), Perceived Financial Risk (PFR), Perceived Fraud Risk (PDR), and Perceived Social Risk (PSoR); with operational definitions sufficient to anchor future scale development.

Materials and Methods

A systematic search was conducted across Scopus and Web of Science. The primary publication window was 2022 to 2026, with targeted supplementary coverage of foundational theoretical and empirical works from 2006 to 2021 where the primary period yielded insufficient theoretical depth for anchoring specific dimensions. The search strategy employed keyword combinations drawn from the review's conceptual domain: ("online risk" OR "digital risk" OR "internet risk" OR "cyber risk") AND ("perception" OR "awareness" OR "cognition" OR "understanding") AND ("dimensions" OR "aspects" OR "factors" OR "elements") AND ("behavior" OR "decision-making" OR "attitude" OR "response") AND ("trust" OR "security" OR "safety" OR "vulnerability"). Titles, abstracts, and keywords were screened iteratively across two rounds; full texts were retrieved for all sources satisfying initial criteria. Inclusion required that sources address online or digital risk perception as a primary construct and contribute empirical evidence, theoretical development, or dimensional analysis relevant to identifying or operationalizing risk perception components in digital contexts. Sources focused exclusively on offline risk, technology addiction without risk perception content, or non-peer-reviewed grey literature was excluded. After full-text screening, more than 70 sources were retained spanning psychology, information systems, marketing, criminology, public health, and educational technology. Among these, 14 studies were selected for the dimensional mapping analysis presented in *Table 1* on the basis of their explicit identification, operationalization, or psychometric

validation of distinct online risk perception dimensions across diverse contexts. Data extraction was organized across four categories: theoretical framework applied; dimensions or risk factors identified; research context and sample characteristics; and conceptual mapping to the proposed five-dimension framework. Throughout, narrative synthesis was employed with tabular data reserved for systematic cross-study comparisons that cannot be efficiently conveyed in prose.

***Table 1**. Dimensional mapping of online risk perception studies (primary 2022–2026, supplemented with foundational works) to the proposed five-dimension framework.*

Study (Year)	Context and Sample	Dimensions Identified	Mapping to ORPS Framework	Dimension(s) Supported
Dempere et al. (2026)	Crowdfunding adoption; multi-country; SEM	5 risk types explicitly named: financial, security, privacy, social, performance risk; all predict adoption negatively	Financial → PFR; Security → PSR; Privacy → PPR; Social → PSoR; Performance → PDR (partial)	PFR, PSR, PPR, PSoR, PDR
Le and Tran (2026)	Online marketplaces; Vietnam; SEM; fraud-focused	5 fraud sub-dimensions: payment credential theft; account takeover; fraud/non-delivery; checkout scam/phishing; refund/dispute failure	Credential theft + phishing → PDR; Account takeover → PSR + PDR; Non-delivery → PFR; Refund failure → PFR + PDR; strongest independent operationalisation of PDR	PDR, PSR, PFR
Siregar et al. (2026)	GrabFood app; Indonesia (n = 300); SEM-PLS; TAM-based	PSR, PPR, PEOU → Trust → Usage Intention; SRMR = .041; all main hypotheses supported	PSR → PSR; PPR → PPR; Trust mediation → PSoR indirect; Indonesian TAM context confirms PPR + PSR salience for ORPS	PSR, PPR
Carbone et al. (2025)	Digital threats + AI; adults; Italy; psychometric scale	Cyber risk dimensions: threat severity, personal vulnerability, dread, catastrophic potential, personal impact	Severity + dread → PSR; Vulnerability → PSR, PDR; Personal impact → PFR, PPR; Extends psychometric paradigm to AI-era threats	PSR, PDR, PFR, PPR
Kožuh and Čakš (2025)	Social media (fact-checking); Slovenia; survey	Risk perception types: personal risk, societal risk; cognitive and emotional dimensions; fear mediates protective behavior.	Personal risk → PPR, PSR; Societal risk → PSoR; Emotional → PSR (dread); Fact-checking → PDR (deception detection)	PPR, PSR, PSoR, PDR
Wang et al. (2025)	Adolescent online risk; systematic review; global	Risk behaviour domains: conduct risk, content risk, contact risk; gender and age moderate risk perception profiles	Conduct → PDR; Content → PPR + PDR; Contact → PSoR + PDR; Gender moderates all dimensions	PDR, PPR, PSoR
Handoko et al. (2022)	E-payment; consumers; Indonesia – Jabodetabek (n = 109); regression	Perceived risk, perceived trust, perceived security → consumer intention; Adjusted R^2 = .771; trust β = .518	Perceived risk → PFR + PDR; Perceived security → PSR; Trust mediation → PSoR (indirect); Indonesian context confirms local relevance	PSR, PFR, PDR, PSoR
Jacobson et al. (2022)	Online behavior, adults, Canada, qualitative + quantitative	Risk shaped by self-perceived internet skills, negative incident experiences, information archiving behavior.	Skills → PSR (moderation); Negative incidents → PPR, PDR; Archiving → PPR (protective)	PPR, PSR, PDR
Yin et al. (2022)	Online medical communities; China; deep neural network + survey	Privacy risk antecedents: trust, service quality, perceived material rewards, privacy concern	Privacy concern → PPR; Trust → PSR; Material rewards → PFR	PPR, PSR, PFR
Schomakers et al. (2019)	Information sensitivity; internet users; Germany (n = 592); quota sampling + survey	3 sensitivity clusters: high, moderate, low; password and financial data rated most sensitive; privacy disposition is the strongest predictor	Password/financial sensitivity → PPR, PFR; Social-identity data sensitivity → PSoR; Cultural variation → cross-cultural ORPS validation	PPR, PFR, PSoR
van Schaik et al. (2018)	Facebook hazards; adults; UK (n = 201); psychometric paradigm; within-subjects	10 psychometric dimensions applied to 16 hazards: dread, catastrophic potential, control, voluntariness, immediacy, knowledge,	Dread + catastrophic → PSR; Information sharing → PPR; Voluntariness → PSoR; Newness → PDR; Precautionary behaviour	PSR, PPR, PSoR, PDR

		newness, benefit, precaution, information sharing	highest for privacy/security hazards	
Byrne et al. (2016)	Internet activities; adults; US; mixed-methods (interview + survey, n = 261)	7 risk factors: informational, social, financial, tools, games, email, miscellaneous; users engage for benefits, not risk understanding	Financial → PFR; Social → PSoR; Informational → PPR, PDR; Users systematically underestimate risk vs. expert assessment	PFR, PSoR, PPR, PDR
Garg and Camp (2012)	End-user online risk; general population; survey + factor analysis	4 dimensions (reduced from 9): time; severity; physical analogue, and control	Severity + time → PFR, PSR; physical analog → PPR; Control → PSR, PDR	PSR, PFR, PPR, PDR
Gabriel and Nyshadham (2008)	E-commerce; adult users; US; survey + EFA	4 dimensions: direness of consequences; ability to control/avoid; observability/immediacy; unfamiliarity of risk	Direness → PSR + PFR; Unfamiliarity → PDR; Observability → PPR; Control → PSR	PSR, PFR, PPR, PDR

Note: PPR = Perceived Privacy Risk; PSR = Perceived Security Risk; PFR = Perceived Financial Risk; PDR = Perceived Fraud/Danger Risk; PSoR = Perceived Social Risk. Mapping is conceptual, based on the authors' reported constructs. EFA = exploratory factor analysis; SEM = structural equation modeling; SEM-PLS = partial least squares SEM.

Results and Discussion

Theoretical bases of online risk perception

The reviewed literature draws on seven distinct theoretical frameworks to conceptualize online risk perception, each emphasizing different structural aspects and grounding different subsets of the proposed dimensions. *Table 2* summarizes these frameworks, their core principles, the dimensions they ground, and representative studies from the 2022–2026 period. Perceived Risk Theory (Featherman and Pavlou, 2003; Mitchell, 1999) is the most widely applied framework and the only one that simultaneously grounds all five proposed dimensions. It conceptualizes risk as a subjective expectation of loss weighted by the probability and magnitude of negative outcomes and conceptualizes each risk type as a facet of an overall perceived risk construct and predicts that each facet independently diminishes trust and adoption intention. Its predictive validity has consistently proven to be consistent in the context of Indonesian digital platforms (Siregar et al., 2026; Handoko et al., 2022), crowdfunding (Dempere et al., 2026), Vietnamese e-commerce (Tran and Vu, 2023), and online education (Pörzse and Kenesei, 2026), which confirms its primacy as the theoretical scaffold for the proposed framework. The psychometric paradigm (Slovic, 1987; Fischhoff et al., 1978) offers the cognitive-dimensional architecture of risk perception: van Schaik et al. (2018) applied ten psychometric dimensions to 16 Facebook hazards rated by 201 British adult users and demonstrated that dread, catastrophic potential, and lack of control are the strongest predictors of risk perception and precautionary behavior in online social networking, directly grounding PSR and PPR and providing the hazard-level measurement logic for their operationalization. Carbone et al. (2025) extended this psychometric approach to AI-related digital threats in an Italian adult sample, independently validating the PSR and PDR dimensions in a new technology context.

***Table 2**. Theoretical frameworks applied to online risk perception research (2022–2026) and the dimensions each grounds.*

Theoretical Framework	Core Principle Applied to Online Risk	Dimension(s) Grounded	Key Studies (2022–2026)
Perceived Risk Theory	Risk = subjective expectation of loss ×	PPR, PSR, PFR, PDR,	Dempere et al. (2026);

(Featherman and Pavlou, 2003; Mitchell, 1999)	magnitude; each risk type constitutes a distinct facet of overall perceived risk predicting avoidance and adoption behaviour	PSoR (all five dimensions)	Siregar et al. (2026); Tran and Vu (2023); Nawi et al. (2021)
Psychometric Paradigm (Slovic, 1987; Fischhoff et al., 1978)	Risk perception structured along cognitive dimensions: dread, novelty, controllability, catastrophic potential, observability; validated for online social networking hazards	PSR (dread, control); PPR (unfamiliarity); PDR (catastrophic potential)	Carbone et al. (2025); Gavrilov and Butynko (2021); van Schaik et al. (2018)
Technology Acceptance Model (Davis, 1989)	Privacy and security risks reduce perceived usefulness and ease of use, functioning as adoption barriers mediated by trust; confirmed in Indonesian digital platform studies	PPR, PSR	Siregar et al. (2026); Thi (2025); Kaur and Sharma (2022); Yang et al. (2015)
Prospect Theory	Potential losses weighted more heavily than equivalent gains; users engage in digital activities for perceived benefit while underestimating financial and fraud risk	PFR, PDR	Le and Tran (2026); Savas-Hall et al. (2022); Byrne et al. (2016)
Theory of Planned Behaviour (Ajzen, 1991)	Subjective norms and social expectations shape risk attitudes; publicly visible digital participation heightens social risk appraisal	PSoR	Dempere et al. (2026); Pörzse and Kenesei (2026); Schomakers et al. (2019)
Information Behaviour Theory (Jacobson et al., 2022)	Prior negative online experiences and self-assessed digital skills dynamically shape risk perception; risk appraisal is experiential, cumulative, and moderated by digital literacy	PPR, PSR (experiential modulation)	Wang et al. (2025); Jacobson et al. (2022); Byrne et al. (2016)
Risk Homeostasis Theory	Users adjust behaviour to maintain subjectively acceptable risk levels; perceived risk systematically diverges from objective exposure in cybercrime and digital contexts	PSR (misperception of actual threat)	Tejamaya et al. (2025); Zeballos Rivas et al. (2021); Vozmediano et al. (2013)

Note: PPR = Perceived Privacy Risk; PSR = Perceived Security Risk; PFR = Perceived Financial Risk; PDR = Perceived Fraud/Danger Risk; PSoR = Perceived Social Risk. TAM = Technology Acceptance Model. The studies listed are representative examples from 2022–2026; foundational works are cited in text.

Extensions of TAM (Siregar et al., 2026; Thi, 2025; Kaur and Sharma, 2022; Davis, 1989) consistently show that PPR and PSR serve as barriers to adoption, negatively impacting perceived usefulness and trust: Siregar et al. (2026) conducted an SEM-PLS study of 300 Indonesian Grab users (SRMR = .041; NFI =.92) that directly confirms these two dimensions as the strongest perceptual predictors of digital platform non-adoption, further confirming their importance in any measurement instrument for Indonesia. Prospect Theory explains the asymmetric influence of PFR and PDR: even small probabilities of financial loss or deceptive outcomes are weighted more heavily than equivalent gains, which Byrne et al. (2016) empirically demonstrated in their seven-factor analysis of 261 US internet users' risk perceptions across 35 online activities in which users systematically underestimated the risks of activities relative to expert security assessments while engaging in them for perceived benefits. The Theory of Planned Behavior (Ajzen, 1991) grounds PSoR through its subjective norm component: in contexts where digital participation is publicly visible and socially evaluated: crowdfunding (Dempere et al., 2026), MOOC enrollment (Pörzse and Kenesei, 2026), and information sharing on social media (Schomakers et al., 2019); the perceived social expectations of significant others moderate engagement decisions in ways that constitute reputational and social identity risks. Information Behavior Theory (Jacobson et al., 2022) establishes that online risk perception is not a fixed trait but is dynamically shaped by cumulative digital experience: users who have encountered negative incidents develop heightened risk sensitivity across PPR and PDR dimensions,

while self-perceived digital skills moderate PSR appraisal, with implications for how ORPS items should be calibrated across digitally diverse adult populations. Risk Homeostasis Theory explains the systematic divergence between perceived and objective online risk documented by Vozmediano et al. (2013) in their cybercrime pilot, where worry about cybercrime (M = 3.73) substantially exceeded perceived risk probability (M = 2.50) across all 11 threat categories, and reaffirmed by Zeballos Rivas et al. (2021) and Tejamaya et al. (2025) in public health risk contexts, establishing the methodological rationale for measuring cognitive probability appraisal rather than affective worry in ORPS.

Dimensions of online risk perception: Mapping the evidence

Table 1 presents the dimensional mapping analysis, in which 14 studies are evaluated for the risk dimensions or factors they identify, operationalize, or psychometrically validate, and each is mapped to the proposed five-dimension framework. The mapping analysis reveals consistent dimensional clustering across independent research traditions and national contexts. PSR and PPR appear in all 14 studies in some form, which reflects their grounding in both perceived risk theory and the psychometric paradigm and their empirical salience across the widest range of online contexts, from Facebook hazards (van Schaik et al., 2018) to Indonesian e-payment (Siregar et al., 2026; Handoko et al., 2022), online medical communities (Yin et al., 2022), crowdfunding (Dempere et al., 2026), and social media fact-checking (Kožuh and Čakš, 2025). PFR appears in 11 of the 14 studies, predominantly in transactional contexts but also in non-transactional digital health settings (Tejamaya et al., 2025; Zeballos Rivas et al., 2021), where resource loss from risk exposure constitutes a financially proximate cost. PSoR appears in 10 studies, with particular salience in social media (Kožuh and Čakš, 2025; Hwang et al., 2025), crowdfunding (Dempere et al., 2026), and MOOC contexts (Pörzse and Kenesei, 2026) where publicly visible participation carries reputational stakes, as well as in the information sensitivity research of Schomakers et al. (2019) and van Schaik et al. (2018), where social-identity-related data are rated most sensitive. PDR, the most theoretically contested dimension, appears explicitly in 9 studies, with the strongest independent operationalization provided by Le and Tran (2026), whose decomposition into five marketplace fraud sub-dimensions: payment credential theft; account takeover; fraudulent non-delivery; checkout scam and phishing; and refund and dispute failure; establishes it as a multi-faceted construct with distinct item content. Byrne et al. (2016), in their foundational seven-factor analysis, independently identified a dimension addressing the misleading, deceptive, and manipulative aspects of online information and interaction that cannot be reduced to financial or security risk, further supporting PDR's status as a dimensionally separable construct. The presence of PDR across five distinct research streams: marketplace fraud (Le and Tran, 2026), social media deception (Kožuh and Čakš, 2025), risk perception measurement (Byrne et al., 2016), cybercrime (Vozmediano et al., 2013), and adolescent online safety (Wang et al., 2025); establishes its cross-contextual validity, even where it has not been independently labeled as a distinct dimension.

Operational definitions of the five dimensions

Building on the theoretical frameworks outlined in *Table 1* and the dimensional evidence presented in *Table 2*, five distinct dimensions are identified and clearly

defined. The first, Perceived Privacy Risk (PPR), refers to an individual's personal belief that sharing data online could result in that information being collected, stored, used, disclosed, or transmitted without permission, potentially leading to identifiable harms such as identity theft, surveillance, or loss of control over personal information. This definition combines elements from the information sensitivity model (Schomakers et al., 2019), longstanding privacy concern research (Choi and Thompson, 2026; Sun et al., 2022), and the privacy-focused psychometric risk profile found by van Schaik et al. (2018) in the context of social networks. The privacy paradox, where users acknowledge privacy risks but still share their information; frequently reported in recent studies (Fejes-Vékássy et al., 2024), highlights why PPR needs to be measured independently from actual privacy-related behaviors. Perceived Security Risk (PSR) is the individual's subjective assessment of the probability that their digital accounts, systems, or data will be compromised by unauthorized third-party access, including hacking, phishing, identity theft, malware, or platform integrity failure. PSR is distinguished from PDR by its focus on system or account vulnerability rather than counterpart deception: the threat agent in PSR is the system-level failure or the generic malicious actor, not a specific deceptive counterpart within a transaction. According to van Schaik et al. (2018), the privacy paradox, where people recognize privacy risks yet still disclose information, has been consistently observed in recent research (Fejes-Vékássy et al., 2024). This ongoing trend underscores why PPR should be treated as a distinct construct, separate from actual privacy behaviors, and measured on its own merits.

Perceived Financial Risk (PFR) is the individual's assessment of the likelihood and magnitude of monetary loss arising from digital activities, including fraudulent transactions, payment credential compromise, failed deliveries, investment loss, and wasted expenditure of monetary resources. PFR is the most consistently reported dimension across the reviewed literature, appearing across all transactional contexts and grounded in both Perceived Risk Theory (the financial loss facet) and Prospect Theory (loss aversion amplifying the psychological weight of even small financial risks). Le and Tran (2026) contribute the important distinction between PFR and PDR at the operational level: whereas PFR covers monetary outcomes, PDR covers the deceptive processes through which those outcomes are brought about. Items targeting PFR should therefore address monetary exposure and financial loss outcomes, not the detection of deceptive intent. Perceived Fraud Risk (PDR) is the individual's subjective probability of encountering deliberate deception by another party in an online environment, including phishing, scam transactions, counterfeit listings, fraudulent information, impersonation, and manipulation. PDR is operationally distinct from PSR (which involves technical system compromise) and from PFR (which involves monetary outcomes) because it involves the cognitive appraisal of a specific type of threat agent: an intentionally deceptive human counterpart within a relational or transactional context. The associated behavioral responses, counterpart verification, skepticism, refusal to initiate contact with unknown parties, and information cross-checking, are behaviorally distinct from the precautionary software and account protection measures associated with PSR. Wang et al. (2025) conducted a comprehensive review of adolescent online risk behaviors, identifying a domain focused on conduct risks that closely aligns with PDR. This includes risks like harmful contacts, exposure to deceptive content, and interactions with unfamiliar individuals, providing evidence that supports the relevance of PDR across different contexts and age groups.

Perceived Social Risk (PSoR) is the individual's subjective assessment of the probability that online activities, disclosures, or participation decisions will result in negative social consequences, including reputational harm, peer disapproval, social relationship disruption, or psychosocial well-being costs arising from social pressure in online interactions. Van Schaik et al. (2018) identified that public exposure of personal or reputational information on platforms like Facebook elicited the highest levels of concern and the strongest preventive actions among users. Similarly, Pörzse and Kenesei (2026) found that worries about non-financial risks, such as reputation and social image, are key reasons people hesitate to enroll in MOOCs, where choices can impact social identity. Further research by Hwang et al. (2025) and Kožuh and Čakš (2025) supports that the perception of societal-level risk, a collective form of PSoR, is a distinct and measurable aspect of how people assess online risks, especially in the realm of social media.

This review compared the main theories, dimensions, and research settings found in studies on online risk perception published between 2022 and 2026, aiming to create a more unified framework for future measurement. The literature shows that researchers use a wide variety of theories, terms, and fields to study online risk perception. However, when these studies are examined together, five key dimensions consistently appear: Perceived Privacy Risk (PPR), Perceived Security Risk (PSR), Perceived Financial Risk (PFR), Perceived Fraud Risk (PDR), and Perceived Social Risk (PSoR). This suggests that differences in previous research are mainly due to varying perspectives and contexts, not because researchers are describing fundamentally different concepts. As a result, the proposed framework offers a way to bring together findings from different approaches into a single, cohesive structure. The analysis of theoretical backgrounds shows that the main theories in this field do not compete with each other but instead address different aspects of online risk perception. For example, perceived risk theory lays the groundwork for understanding the multi-faceted nature of risk (Featherman and Pavlou, 2003; Mitchell, 1999). The psychometric paradigm looks at how people think about online dangers based on factors like dread or familiarity (Slovic, 1987; Fischhoff et al., 1978). The Technology Acceptance Model focuses on how risk affects decisions to adopt technology (Davis, 1989), while Prospect Theory addresses how people weigh financial losses. Other theories like the Theory of Planned Behavior, Information Behavior Theory, and Risk Homeostasis Theory each add further layers, covering social influence, past experiences, and why perceived risk might not match actual risk. Together, these theories give a fuller picture of how people perceive and respond to online risk.

This broader perspective is important for developing a better framework. Many past studies have used these theories separately, which has led to fragmented ideas and inconsistent ways of measuring online risk perception. By combining their strengths, the framework in this review builds a more solid theoretical basis for the five main dimensions. Instead of using just one lens, this approach shows why privacy, security, financial, fraud, and social risks are repeatedly found as the core types of online risk perception in many contexts. Looking at the main dimensions, the literature reveals a strong pattern, even though different terms and methods are used. Studies in areas like e-commerce, social media, crowdfunding, digital banking, online education, healthcare, and online marketplaces almost always identify risks that can be grouped into the same five categories. This shows that variations in previous work mostly reflect the area of study or theoretical focus, rather than suggesting that the fundamental ideas are

different. Among these, privacy and security risks are the most common concerns across different fields. Whether the focus is on e-commerce, crowdfunding, social media, or digital health, users consistently worry about issues like sharing personal information, unauthorized access to data, cyberattacks, identity theft, and how secure a platform is (Dempere et al., 2026; Choi and Thompson, 2026; Kumar and Gupta, 2020; van Schaik et al., 2017; Lee and Huddleston, 2010). This suggests that privacy and security are central to how people judge whether a digital environment is safe and trustworthy.

Financial and social risks also appear regularly, but their importance changes depending on the context. Financial risk is more pronounced in settings with online transactions, such as crowdfunding or digital banking, where the fear of losing money directly affects trust and decision-making (Dempere et al., 2026; Nawi et al., 2021; Yang et al., 2014). Social risk, meanwhile, stands out more in spaces where public interaction matters, like social media or online learning, as decisions often relate to reputation, peer pressure, or social identity (Dempere et al., 2026; Pörzse and Kenesei, 2026). These variations are shaped by the research context, not by fundamental disagreements about the core dimensions. Recognizing Perceived Fraud Risk (PDR) as a separate category is also justified. Many studies have combined fraud with either security or financial risks, since fraud often involves both technical and financial issues (Dempere et al., 2026; van Schaik et al., 2017). However, the evidence suggests that fraud is best understood as a distinct concern, one that is specifically about deception. For example, Le and Tran (2026) list types of fraud like payment credential theft and phishing, which go beyond just technical or financial problems. Wang et al. (2025) further show that people respond to fraud with behaviors, such as double-checking information, that are different from how they respond to general security or financial risks. This supports the view that PDR is an independent dimension, though it is closely linked to the others.

Examining different research contexts confirms that the five-dimensional framework applies to a range of digital environments, including e-commerce, social media, digital banking, crowdfunding, education, healthcare, and online marketplaces. While each area highlights certain risks more than others, all of the key dimensions can be found in every context. This shows that the main structure of online risk perception is flexible and widely applicable (*Table 2*). Similarly, instruments used to measure online risk perception, such as the Internet Risk Perception Scale (Torres-Hernández et al., 2022), the Online Risk Scale (Kanetsuna et al., 2023), the Cybercrime Risk Perception Questionnaire (Vozmediano et al., 2013), and the Virtual World Risk Perception Scale (Arslankara and Usta, 2018); reflect different priorities and backgrounds. For instance, some focus mainly on privacy or security, while others lack financial or fraud dimensions. This shows that existing tools are tailored to particular contexts, rather than providing a consistent model of online risk perception. Based on these findings, there is a strong case for developing a unified measurement tool. The new Online Risk Perception Scale (ORPS) proposed here combines evidence from different disciplines and research settings, offering a thorough conceptual base for future work. It promises better coverage of all the main dimensions and greater consistency across studies, making it easier to compare results and build stronger theories. Future research should focus on testing and validating the ORPS in various cultures and settings, since most current studies focus on Western or East Asian populations. There are some limitations to this review. First, although the main period studied was 2022–2026, older key studies were included for their important insights. Second, the way dimensions are grouped in

Table 2 is the result of the authors' interpretation, and others might group them differently. Lastly, the framework was developed by comparing studies, not from a single theory, which means further testing is needed to confirm its reliability in different contexts.

Conclusion

This systematic review of the online risk perception literature from 2022 to 2026 makes three contributions. It provides an integrated mapping of seven theoretical frameworks and their differential contribution to the conceptualization of online risk perception, demonstrating for the first time that these frameworks are complementary rather than competing and that their synthesis provides comprehensive multi-level theoretical grounding for a five-dimension model. It presents a dimensional mapping analysis of 14 primary studies that establishes PPR, PSR, PFR, PDR, and PSoR as the five cross-contextually robust dimensions of online risk perception, with particular attention to the process-centered argument for PDR's independence from PSR and PFR. And it provides operational definitions for each of the five dimensions that are grounded in the reviewed theoretical and empirical literature and are sufficient to anchor future scale development. Together, these contributions establish the conceptual foundation for a dedicated Online Risk Perception Scale (ORPS) capable of measuring all five dimensions in a unified, psychometrically validated instrument. The next research priority is the development and validation of such an instrument through expert content validation using Content Validity Index procedures, exploratory factor analysis with a diverse adult internet user sample, and confirmatory factor analysis with a second independent sample, examining both first-order dimension structure and second-order general factor structure consistent with perceived risk theory. Cross-cultural validation should follow, with particular attention to contexts, including Southeast Asian digital economies with distinct cultural risk profiles; where the framework has not yet been empirically tested.

Acknowledgement

This research is self-funded.

Conflict of interest

The authors confirm that there is no conflict of interest involve with any parties in this research study.

REFERENCES

[1] Ajzen, I. (1991): The theory of planned behavior. – Organizational Behavior and Human Decision Processes 50(2): 179-211.
[2] Arslankara, V.B., Usta, E. (2018): Development of Virtual World Risk Perception Scale (VWRPS). – Bartın University Journal of Faculty of Education 7(1): 111-131.
[3] Arruda Filho, E.J.M., Gammarano, I.D.J.L.P., Duarte, E.M.C. (2023): Smile, you're being watched: Digital privacy and risk perception regarding data sharing on social networks. – Interacting with Computers 35(1): 12-23.

[4] Byrne, Z.S., Dvorak, K.J., Peters, J.M., Ray, I., Howe, A., Sanchez, D. (2016): From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet. – Computers in Human Behavior 59: 456-468.
[5] Carbone, D., Marcatto, F., Mistichelli, F., Ferrante, D. (2025): Perceiving digital threats and artificial intelligence: A psychometric approach to cyber risk. – Journal of Cybersecurity and Privacy 5(4): 17p.
[6] Choi, S., Thompson, L. (2026): Exploring the impact of media awareness on privacy concerns among social media users: A case study of TikTok. – Journal of Applied Security Research 21(1): 112-137.
[7] Davis, F.D. (1989): Perceived usefulness, perceived ease of use, and user acceptance of information technology. – MIS Quarterly 13(3): 319-340.
[8] Dempere, J., Allam, H., Udjo, E., Becermen, O., Harris, J. (2026): The role of perceived risk in the adoption of crowdfunding platforms: A comprehensive analysis. – Advances in Science, Technology and Innovation, Springer 13p.
[9] Featherman, M.S., Pavlou, P.A. (2003): Predicting e-services adoption: A perceived risk facets perspective. – International Journal of Human Computer Studies 59(4): 451-474.
[10] Fejes-Vékássy, L., Ujhelyi, A., Lantos, N.A. (2024): I don't care, I share! The importance of self-disclosure overwrites the risks of sharing on social media. – Current Psychology 43(38): 30120-30134.
[11] Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B. (1978): How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. – Policy Sciences 9(2): 127-152.
[12] Gabriel, I.J., Nyshadham, E. (2008): A cognitive map of people's online risk perceptions and attitudes: An empirical study. – Proceedings of the Annual Hawaii International Conference on System Sciences 10p.
[13] Garg, V., Camp, J. (2012): End user perception of online risk under uncertainty. – Proceedings of the Annual Hawaii International Conference on System Sciences 9p.
[14] Gavrilov, K.A., Butynko, M.V. (2021): The perception of cyber and traditional risks: Experience of using the psychometric paradigm approach. – Sotsiologicheskiy Zhurnal 27(4): 146-168.
[15] Handoko, B.L., Siswono, Azani, J.M. (2022): Analysis of perceived risk, perceived trust, perceived security factors on consumer intention using e-payment. – Proceedings of the 2022 8th International Conference on E-business and Mobile Commerce (ICEMC 2022), ACM 8p.
[16] Hwang, H., Kim, K., Lee, C.-J., Kang, B.-A., Lee, H. (2025): An integrative analysis of psychological mechanisms underlying the effects of online and social media exposure on drought mitigation-related outcomes. – Risk Analysis 45(11): 3585-3603.
[17] Jacobson, J., Lin, C.Z., McEwen, R. (2022): Information behaviour paradox: Understanding perceptions of risk and online behaviour. – Library and Information Science Research 44(4): 10p.
[18] Kanetsuna, T., Ieshima, A., Toda, Y. (2023): Development of an online risk scale for high school students. – Psychology 14: 1810-1826.
[19] Kaur, B., Sharma, R.R. (2022): Factors affecting behavioural intentions to use e-banking services: An extension of TAM in Indian context. – International Journal of Business and Globalisation 32(4): 414-430.
[20] Kožuh, I., Čakš, P. (2025): Understanding social media behaviour: The role of risk perception in crowdsourced fact-checking. – SAGE Open 15(4): 12p.
[21] Kumar, M., Gupta, S. (2020): Security perception of e-banking users in India: An analytical hierarchy process. – Banks and Bank Systems 15(1): 11-20.
[22] Le, D.V., Tran, H.M.N. (2026): Fraud risk perception and online payment choice model on online marketplaces: Evidence from the Mekong Delta, Vietnam. – Proceedings of the 2026 18th International Conference on Electronics, Computer, and Computation (ICECCO 2026) 8p.

[23] Lee, H.-J., Huddleston, P.T. (2010): An investigation of the relationships among domain-specific innovativeness, overall perceived risk and online purchase behaviour. – International Journal of Electronic Marketing and Retailing 3(1): 1-14.
[24] Mitchell, V. (1999): Consumer perceived risk: Conceptualisations and models. – European Journal of Marketing 33(1-2): 163-195.
[25] Nawi, N.B.C., Mamun, A.A., Md Nasir, N.A., Hamsani, N.H.B. (2021): Examining the risk factors affecting the image of online stores in Malaysia. – International Journal of Electronic Marketing and Retailing 12(2): 156-170.
[26] Pörzse, G., Kenesei, Z. (2026): To enrol or not to enrol: What are the risks in choosing a massive open online course (MOOC)? – International Review of Education 72(2): 345-367.
[27] Savas-Hall, S., Koku, P.S., Mangleburg, T. (2022): Really new services: Perceived risk and adoption intentions. – Services Marketing Quarterly 43(4): 485-503.
[28] Schomakers, E.-M., Lidynia, C., Müllmann, D., Ziefle, M. (2019): Internet users' perceptions of information sensitivity: Insights from Germany. – International Journal of Information Management 46: 142-150.
[29] Siregar, M.Y., Mahrinasari, M.S., Roslina (2026): The effect of perceived usefulness, perceived security risk, perceived privacy risk, and perceived ease of use on trust and usage intention of the GrabFood Dine-Out Deals feature in Indonesia. – International Journal of Economics, Business and Innovation Research 5(1): 148-160.
[30] Slovic, P. (1987): Perception of risk. – Science 236(4799): 280-285.
[31] Sun, Z., Zhao, H., Zang, G., Wang, Z. (2022): Research on privacy disclosure intention of social commerce users based on a dual calculus perspective. – Library and Information Service 66(24): 64-75.
[32] Tejamaya, M., Putri, A.A., Widanarko, B., Wirawan, I.M.A., Kurniawan, B., Thamrin, Y. (2025): Dynamics of COVID-19 risk perception in Indonesia: A consecutive cross-sectional study from 2020 to 2022. – Safety and Health at Work 16(4): 421-430.
[33] Thi, T.D.P. (2025): Investigating factors of loyalty intention among m-banking users: An integrated model. – International Journal of Procurement Management 22(2): 261-280.
[34] Torres-Hernández, N., García-Martínez, I., Gallego-Arrufat, M.-J. (2022): Internet risk perception: Development and validation of a scale for adults. – European Journal of Investigation in Health, Psychology and Education 12: 1581-1593.
[35] Tran, H.M.N., Vu, D.L. (2023): The influence of risk perception on online shopping decision of consumers: A case study of social media platforms in Vietnam. – ACM International Conference Proceeding Series 6p.
[36] Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., Kusev, P. (2018): Security and privacy in online social networking: Risk perceptions and precautionary behaviour. – Computers in Human Behavior 78: 283-297.
[37] Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., Kusev, P. (2017): Risk perceptions of cyber-security and precautionary behaviour. – Computers in Human Behavior 75: 547-559.
[38] Vozmediano, L., San-Juan, C., Vergara, A.I., Lenneis, A. (2013): Risk perception in digital contexts: Questionnaire and pilot study. – International e-Journal of Criminal Science 7: 10p.
[39] Wang, L., Wang, W., Fei, W., Wang, Z. (2025): Online risk behavior in adolescents: A systematic review. – Trauma, Violence, and Abuse 15p.