Advances in Consumer Research
https://acr-journal.com/
Volume-3 | Issue-3 | March 2026
Original Researcher Article

Risk Before Trust: How Consumers Authorise Digital Credit Under Cyber Threats

Ratnakumar Pullagura [1*], Dr. Priti Bakhshi [2], Dr. Anshul Gupta [3]
[1]Affiliations: DBA Research Scholar, SP Jain School of Global Management, Sydney, Australia
ratnakumar.dj24dba004@spjain.org
ORCID ID: 0009-0005-0326-7952
[2]Affiliations: Professor, SP Jain School of Global Management, Mumbai, India
(priti.bakhshi@spjain.org)
[3]Affiliations: Associate Professor, SP Jain School of Global Management, Dubai, UAE
(anshul.gupta@spjain.org..

ABSTRACT
Digital finance research has long assumed that trust is the primary mechanism enabling consumer participation in online markets. We challenge this assumption in the context of embedded digital credit by proposing the Heuristic Authorisation Model (HAM), which argues that in threat-salient, low-deliberation environments, consumers authorise financial exposure through vulnerability-reduction heuristics rather than relational trust. When credit is embedded at checkout and decisions unfold within seconds, perceived exposure not institutional belief governs behavioural thresholds. Using survey data from 150 Buy Now Pay Later (BNPL) users in Australia, a high cybersecurity-salience market, we test whether perceived cybersecurity influences authorisation through trust formation or through reductions in perceived vulnerability. Results show that perceived cybersecurity increases both trust and perceived risk reduction; however, only perceived risk reduction significantly predicts authorisation intention. The indirect effect operates primarily through perceived vulnerability rather than relational trust. These findings suggest that, in embedded credit contexts, vulnerability appraisal may function as a more proximal determinant of authorisation than trust..
Keywords: Heuristic Authorisation Model; digital credit; embedded finance; perceived cyber threat; perceived risk; trust; vulnerability appraisal; consumer decision-making; fintech adoption; BNPL

INTRODUCTION:

Digital marketplaces are increasingly designed to compress consumer decision-making. Consumers now evaluate, select, and commit under conditions shaped by speed, information overload, personalisation, and interface cues rather than extended deliberation [4, 26, 53]. This shift matters most when the decision involves **authorizing financial exposure**. When financial decisions are embedded into consumption moments, the consumer's task is not simply to "adopt" a technology; it is to **cross an exposure threshold** under uncertainty [11, 31].

At the same time, digital life is characterized by persistent perceptions of vulnerability. Consumers face ongoing cues about surveillance, fraud, data misuse, and algorithmic opacity, which elevate perceived threat and coping concerns [25, 46, 27]. Prior work shows that perceived threat changes behaviour by triggering protective responses and shifting attention toward risk and coping rather than value maximisation [8, 15, 27]. This combination **decision compression + perceived cyber threat** raises a fundamental question for consumer research: *what psychological mechanism drives authorisation when exposure feels salient?*

Most digital participation models assume a trust-first logic: trust reduces uncertainty, mitigates perceived risk, and enables intention or continuance [17, 33, 35, 48]. Despite the dominance of trust-based digital participation models, little research has examined whether trust remains behaviourally operative in embedded, threat-salient financial environments. Consumer decision science shows that under load and stress, people shift toward simplified rules and heuristics to reduce cognitive effort [18, 32, 36]. This implies that when consumers authorise digital credit under perceived cyber threat, the operative mechanism may not be relational trust. It may be **vulnerability reduction**, a heuristic evaluation of whether exposure is tolerable.

We propose the **Heuristic Authorisation Model (HAM)**: in threat-salient, compressed decision environments, consumers authorise exposure through vulnerability-reduction heuristics rather than trust-based relational evaluation. In this model, cybersecurity perceptions operate primarily by reducing perceived risk and emotional exposure [6, 16, 30, 48] which then enables authorisation. Trust may increase, but it does not necessarily drive the behavioural threshold [12, 15, 33]. We examine whether perceived vulnerability functions as a more proximal predictor of authorisation intention than relational trust in embedded credit contexts.

This research contributes by identifying a boundary condition for trust-centric digital decision models and by reframing "adoption" as **authorisation**: a threshold act

under perceived vulnerability [1, 11, 52]. More broadly, it links modern digital decision architectures personalisation, information complexity, cognitive load to exposure-based heuristics in security-salient environments [14, 19, 23, 53].

Theoretical Framework and Development of the Heuristic Authorisation Model (HAM)

Digital Decision Compression and Exposure-Based Evaluation

Consumer decision strategies vary with respect to situation and context. Under increased time pressure, complexity and cognitive load, consumers tend to rely on more expedient decision-making procedures and make use of more decision-making heuristics [18, 32]. The virtual environment can also be seen as a context that increases constraints on consumer decision-making. The on-line buying process shortens the time required to buy, provides customer services tailored to the individual's needs, decision-support tools that are highly focused and generally allow for a smoother buying experience [4, 19, 23, 53]. In any case, the complexity of the consumer's deliberation process as well as the extent to which consumers engage in more systematic institutional evaluations of the shops considered will probably decrease. Consumers are increasingly being asked to decide on financial issues while engaged in a primary shopping activity. Exposing consumers' financial resources within the shopping environment (i.e. before they have taken a final buying decision about the product attributes) requires them to act as 'principal authors' who "agree" or "contract" to possible exposure to loss in case of unknown or uncertainty about a possible loss in case of the purchase at stake. The assumption that this authorisation is grounded on trust might not be verified.

Risk, Vulnerability, and Affective Processing

Risk in consumer behaviour has both cognitive and affective elements. Consumer perceived risk refers to the extent to which consumers believe that they may lose something of value because of their purchase decision and are therefore susceptible to a potential threat [12, 34, 50]. An affective response to risk (i.e. anxiety, fear) is an important factor in determining consumers' level of exposure to risky situations [6, 13, 30, 46]. As per protection motivation theory, the presence of threat cues in the environment will draw the consumer's attention away from their preferred goal of achieving maximum satisfaction and direct it towards protection and coping activities [15, 24, 27]. In general, consumers' perceived risk of online shopping has been shown to deter purchases in numerous studies [8, 9, 54]. High levels of emotional risk can increase consumer resistance through avoidance behaviour [3, 6]. Consumers with high emotional risk are more concerned with coping and dealing with risk and therefore are less focused on reducing their exposure to the risk and are therefore less likely to engage in purchase related deliberations, thereby neglecting social aspects of online purchasing behaviour.

Trust as the Dominant Model and It's Boundary

Trust frameworks have been an area of focus for us in our research into digital participation. Research into trust has shown that trust mitigates uncertainty, which in turn affects behavioural intention and continuance [17, 33, 35]. Another related finding is that trust can be transferred from one platform to another [29], and that trust also strongly influences online behaviour [22]. The problem here is that the trust theory assumes that there are sufficient cues to allow us to make relational inference and institutional evaluation. Our research has however revealed that the conditions for trust to have an operative effect are weakened in situations where decision-making is compressed and the cues available for evaluation are reduced or non-existent. We know from previous research that when people are under high levels of cognitive load, they are forced to rely on more simplistic decision-making heuristics when time for decision-making is constrained [14, 19, 32]. So here trust may be formed at a cognitive level but does not have a behavioural effect as the individual does not pass the relevant behavioural threshold. So, our research does not challenge the validity of the trust theory but instead identifies a boundary condition where the trust is less behaviourally operative in situations where there is decision compression, and where the individual is in a highly vulnerable situation.

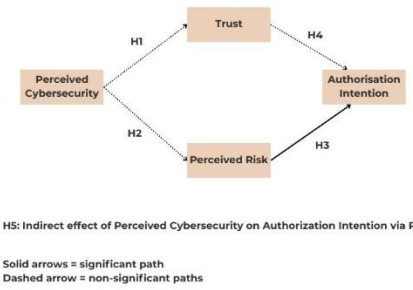
Authorisation as Threshold-Based Commitment

Authorisation intention refers to the intention to authorise accepting risk in uncertain situations. While the studies of adoption, continuance, threshold decisions, preference formation and decision avoidance and no-choice preference have been examined thoroughly in literature, in this study the authorisation intention is investigated. Hence, it can be concluded that authorisation is a threshold-based decision, and it does not belong to the preference formation and decision avoidance and no-choice preference research stream [7, 11, 31]. In the exposure-based context, this study examined if the consumers think that their exposure level falls within the acceptable range of their vulnerability.

The Heuristic Authorisation Model (HAM)

The Heuristic Authorisation Model proposes that when (1) decision environments are compressed and (2) perceived threat is salient, consumers rely on vulnerability-reduction heuristics to authorise exposure.

Figure 1. The Heuristic Authorisation Model (HAM)



Specifically:

Perceived cybersecurity cues reduce perceived vulnerability [8, 39, 48].

Reduced vulnerability enables authorisation intention to increase.

Trust may increase alongside perceived safety [17, 33], but it does not necessarily drive authorisation.

In this framework, the operative psychological sequence shifts from:

Trust → Risk → Behaviour

to:

Risk Reduction → Authorisation

Trust remains present but secondary. HAM therefore identifies a boundary condition for trust-centric digital decision models. Under embedded, time-compressed, threat-salient conditions, vulnerability appraisal dominates relational evaluation. While the present study does not directly measure heuristic processing, the model draws on dual-process and adaptive decision-making frameworks to theorize that embedded credit environments may elevate the relative influence of vulnerability appraisal. The empirical test focuses on comparative mediation rather than on cognitive-process verification.

Hypotheses

H1: Perceived cybersecurity increases trust.
H2: Perceived cybersecurity reduces perceived risk.
H3: Reduced perceived risk increases authorisation intention.
H4: Trust does not significantly predict authorisation intention in embedded credit contexts.
H5: The relationship between perceived cybersecurity and authorisation intention is mediated by perceived risk rather than trust.

Methodology

Research Context

The Heuristic Authorisation Model (HAM) was empirically tested in the context of embedded digital credit where financial exposure is authorised within the retail interface rather than within the broader institutional relationships. We refer to several psychological phenomena which describe environments like ours as being characterised by cognitive compression, interface-based cues and shallow social relationships [4, 14, 19]. Since consumers often use heuristic-based decision-making in situations where they are under pressure, and/or where a system is highly complex [19, 32, 43], we argue that embedded digital credit is an appropriate context in which to investigate the factors that influence authorisation intention, namely relational trust versus vulnerability-reduction.

3.2. Sample and Procedure

Data were collected using an online survey from active users of an embedded digital credit product. Only users who had authorised digital credit in the last 12 months were eligible to complete the survey. After screening and attention checks, valid survey data were collected from 150 active users. We considered this sample size sufficient for mediation analysis according to the structural equation modelling literature [37, 38]. The survey was undertaken in an anonymous and voluntary fashion with all participants providing their informed consent.

3.3. Measures

All constructs were measured using multi-item scales adapted from established consumer and digital trust literature.

Perceived Cybersecurity: We have seen that consumer concern for cybersecurity was an important dimension. Perceived Cybersecurity refers to the consumer belief that a given platform will effectively safeguard sensitive personal and financial information. Like with perceived environmental safety and threat mitigation cues discussed in [25, 46], here we see this concept in the context of digital systems.

Trust: Trust in the context of electronic commerce refers to the faith that consumers have in the availability of certain electronic commerce services and the reliability and integrity of providers. Here, our definition of trust follows that in the literature of digital trust [17, 33, 35].

Perceived Risk: Consumer credit risk related to potential financial loss, data breach or adverse consequence because of lending. It refers to the cognitive and affective aspects of risk evaluation as mentioned in the literature [8, 47, 48]. The codes for this construct are the reverse of those used in the analysis, so that high scores represent low levels of this construct and are discussed in terms of vulnerability reduction.

3.4. Authorisation Intention

Authorisation intention was defined as the consumer's intention to authorise pay later to increase access to cash for purchases where the amount is not certain. Based on the theoretical framework this construct is linked to the threshold-based commitment decision which falls under the umbrella of decision avoidance and exposure tolerance research [1, 11, 31]. All items were measured using 5-point Likert scales with responses ranging from 1 (strongly disagree) to 5 (strongly agree).

3.5. Analytical Strategy

To test the Heuristic Authorisation Model, we estimated a structural model examining:

The effect of perceived cybersecurity on trust and perceived risk.

The effects of trust and perceived risk on authorisation intention.

The indirect effects of perceived cybersecurity on authorisation intention through both mediators.

Bootstrapping procedures were used to assess indirect effects and mediation strength [28, 38]. Our theoretical focus was comparative mediation: whether perceived risk serves as the primary pathway linking cybersecurity perceptions to authorisation intention, relative to trust. This analytical structure allows a direct empirical test of HAM's core claim: that vulnerability reduction, rather than relational trust, governs authorisation under

conditions of perceived digital threat and cognitive compression [14, 19, 20].

Results

4.1. Overview

The central test of the Heuristic Authorisation Model (HAM) was whether perceived cybersecurity influences authorisation intention primarily through relational trust or through reductions in perceived vulnerability. The results clearly favour the vulnerability pathway.

4.2. Cybersecurity, Trust, and Perceived Risk

Consistent with prior trust-based models of digital exchange [17, 33], perceived cybersecurity significantly increased trust. Consumers who believed the platform employed strong security protections reported greater confidence in its reliability.

Perceived cybersecurity also significantly reduced perceived risk, indicating that security cues functioned as exposure-dampening signals. This finding aligns with risk and affective vulnerability frameworks suggesting that safety cues reduce both cognitive and emotional exposure concerns [8, 40, 41].

Notably, the magnitude of the cybersecurity → perceived risk pathway exceeded that of the cybersecurity → trust pathway. This suggests that consumers interpret cybersecurity cues primarily as mechanisms of vulnerability reduction rather than purely as relational assurances.

Path	β	p-value	Hypothesis	Result
Cybersecurity → Trust	0.85	<0.001	H1	Supported
Cybersecurity → Perceived Risk	-0.87	<0.001	H2	Supported
Perceived Risk → Authorisation	-0.36	<0.001	H3	Supported
Trust → Authorisation	0.08	--	H4	Not Supported

Table 1. Structural Path Estimates

4.3. Predicting Authorisation Intention

Perceived risk strongly predicted authorisation intention. As vulnerability decreased, consumers were more willing to grant permission to accept financial exposure. This is consistent with research showing that affective risk perceptions and threat appraisal shape behavioural thresholds under uncertainty [3, 39, 54].

In contrast, trust did not significantly predict authorisation intention once perceived risk was included in the model. Although trust increased alongside perceived cybersecurity, it did not cross the behavioural threshold required for authorisation. This directly supports HAM's boundary condition argument: trust may exist cognitively, but it does not necessarily drive behaviour in compressed, threat-salient contexts.

4.4. Mediation Analysis

When both mediators were included simultaneously, only perceived risk remained a significant predictor of authorisation intention. The indirect pathway through trust was not significant.

These findings indicate that perceived cybersecurity influences authorisation primarily by reducing perceived vulnerability rather than by strengthening relational confidence. In other words, consumers authorise digital credit when they feel less exposed not because they feel more trusting.

4.5. Theoretical Interpretation

Taken together, the results support a reordering of psychological sequence. Under conditions of digital decision compression [14, 42, 44] and perceived threat salience [27, 45] authorisation appears to be governed by vulnerability appraisal rather than by relational trust evaluation. Trust formation is present but behaviourally secondary. Vulnerability reduction is operative. This empirical pattern provides direct support for the Heuristic Authorisation Model.

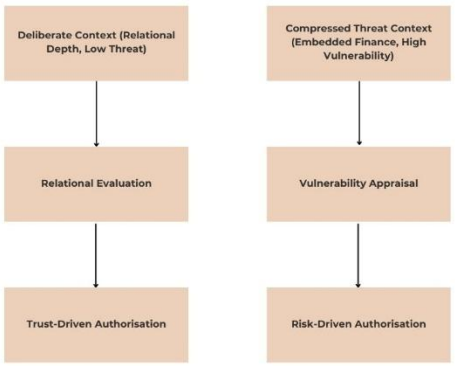
Discussion

5.1. Risk Before Trust: A Boundary Condition for Digital Trust Models

Digital participation research has largely treated trust as the central mechanism enabling online exchange [17, 35, 49]. Our findings qualify that assumption. Although perceived cybersecurity significantly increases trust, trust does not drive authorisation intention in embedded digital credit contexts. Instead, reductions in perceived vulnerability fully account for the pathway from cybersecurity perception to authorisation.

These findings suggest that in embedded credit contexts, vulnerability appraisal may be more proximally associated with authorisation intention than trust. This refines trust-based models by highlighting contextual variation in mechanism dominance. In environments characterized by cognitive compression [14, 51, 55] and heightened vulnerability salience [21, 27], consumers appear to rely on exposure-based heuristics rather than relational evaluation. Trust may coexist with authorisation, but it does not determine the behavioural threshold.

Figure 2. Boundary Condition of the Heuristic Authorisation Model



The theoretical shift is subtle but important: the operative question in authorisation is not "Do I trust this provider?" but "Is my exposure acceptable?"

5.2. The Heuristic Authorisation Model (HAM)

The Heuristic Authorisation Model formalizes this shift. HAM proposes that when (1) decision environments are compressed and (2) threat salience is elevated, consumers rely on vulnerability-reduction heuristics to authorise exposure.

The process unfolds as follows:

Cybersecurity cues reduce perceived vulnerability. Security signals function as coping mechanisms that attenuate exposure concerns [8, 39, 48].

Reduced vulnerability enables threshold crossing. Authorisation reflects a commitment decision under uncertainty, consistent with decision avoidance and threshold theories [1, 11, 31].

Trust remains secondary. While trust may increase alongside perceived safety, it does not necessarily drive authorisation in compressed environments [14, 32].

HAM therefore reframes digital credit participation as an act of vulnerability management rather than relational commitment.

5.3. Embedded Finance as Decision Architecture

A broader implication concerns marketplace structure. Embedded digital credit alters the architecture of decision-making. When financial exposure is integrated directly into consumption interfaces, deliberative evaluation narrows. Interface cues substitute for extended institutional assessment. Under these conditions, consumers adapt by relying on simplified heuristics [19, 37, 38]. This structural compression increases the salience of exposure appraisal. Emotional and affective components of risk become more influential in guiding behaviour [2, 3, 6]. The rise of digital personalisation and complex online environments further amplifies reliance on simplified decision rules [5, 23, 53]. In short, marketplace architecture shapes cognitive strategy.

5.4. Theoretical Contributions

This research contributes to consumer theory in three ways.

Relative Mechanism Clarification
This research demonstrates that in embedded digital credit contexts, perceived vulnerability reduction is more strongly associated with authorisation intention than relational trust. This refines trust-based models by identifying conditions under which trust may not be the most proximal predictor of financial authorisation.

Authorisation as Threshold-Based Construct
We distinguish authorisation intention from generic adoption or continuance by conceptualizing it as a threshold-based decision involving acceptance of exposure under uncertainty.

Cybersecurity as Risk Signal
We show that perceived cybersecurity functions not only as a trust-building signal but also as a vulnerability-reduction cue that influences behavioural intention indirectly.

Limitations and Future Research

We do not manipulate or measure the hypothesised influencing conditions. Thus, our findings relate to mechanism dominance within an embedded credit context rather than to the underlying psychological processes. Future experimental work could potentially manipulate decision time, cognitive load or threat cues. The existence of heuristic processing is inferred from the structural properties of the models and has not been directly measured. Experimental manipulation of cognitive load [7, 19], decision time or threat salience [10, 27] might reveal that trust regains its dominance in low threat or low compression conditions. Our results are based on embedded digital credit contexts and may change when people have more time to think about their more deliberative choices. Future studies could explore this boundary more systematically [17, 35]. It would also be valuable to experimentally separate the cognitive and affective components of risk. The affective aspect of risk such as the emotional aspect of feeling vulnerable [6, 39] might be more closely related to the authorisation decision than the cognitive risk assessment.

Conclusion

Digital markets increasingly require consumers to authorise financial exposure under conditions of speed, cognitive compression, and persistent cyber threat salience. The present findings indicate that, in such environments, authorisation intention is governed less by relational trust and more by perceived vulnerability. Consistent with the Heuristic Authorisation Model, perceived cybersecurity influences authorisation primarily by reducing perceived risk, enabling consumers to cross an exposure threshold; trust may increase concurrently, but it does not determine the behavioural outcome. These results refine trust-centric models of digital participation by identifying a boundary condition under which vulnerability appraisal dominates relational evaluation. By conceptualizing authorisation as a threshold-based commitment under uncertainty, this research advances consumer decision theory and highlights how evolving digital architectures reshape the psychological mechanisms underlying marketplace participation.

Declarations

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Ethical Approval

The study was conducted in accordance with institutional research ethics standards. The research protocol complied with applicable guidelines for research involving human participants.

Informed Consent

Informed consent was obtained from all individual participants included in the study. Participation was voluntary and anonymous.

Data Availability

The datasets generated and analysed during the current study are available from the corresponding author on reasonable request.

Acknowledgements

The authors thank the study participants for their time and responses. The authors also sincerely thank Ms. Frezy Johnson Koonan, Secondary School Teacher, for her careful proofreading, editing and valuable feedback on the manuscript. No additional institutional or financial support was received..

REFERENCES

1. Anderson, C. J. (2003). The psychology of doing nothing: Forms of decision avoidance result from reason and emotion. Psychological Bulletin, 129(1), 139–167. https://doi.org/10.1037/0033-2909.129.1.139
2. Bang, H.-S., Kim, D., & Yoo, J. (2024). Consumer trust in AI recommender systems: Impact of perceived fairness and transparency risks. Decision Support Systems, 181, 114293.
3. Bauer, R. A. (1960). Consumer behaviour as risk taking. In R. Hancock (Ed.), Dynamic marketing for a changing world (pp. 389–398). American Marketing Association.
4. Bettiga, D., Lamberti, L., & Cavacece, Y. (2023). Digital channels and consumer decision journeys: Mental representation and choice. Journal of Interactive Marketing, 60, 115–132.
5. Bettman, J. R., Luce, M. F., & Payne, J. W. (1998). Constructive consumer choice processes. Journal of Consumer Research, 25(3), 187–217. https://doi.org/10.1086/209535
6. Braga, A. O., & Simon, G. L. (2021). Emotions, risk perception, and decision making under uncertainty. Journal of Behavioural Decision Making, 34(5), 867–882. https://doi.org/10.1002/bdm.2241
7. Calder, B. J., & Malthouse, E. C. (2020). New frontiers in consumer decision science. Journal of Consumer Psychology, 30(3), 373–377. https://doi.org/10.1002/jcpy.1208
8. Chen, X., Chen, Y., & Wang, R. (2022). Perceived risk and consumer protective behaviours in online shopping. Journal of Business Research, 141, 66–76. https://doi.org/10.1016/j.jbusres.2022.01.019
9. Cui, Y., Wu, J., & Ramesh, V. (2022). Impact of emotional risk on online choice patterns. Journal of Business Research, 144, 336–346. https://doi.org/10.1016/j.jbusres.2022.01.070
10. Delgado-Ballester, E., & Cuestas, P. J. (2021). Value perceptions and decision rules in online choice. Journal of Business Research, 136, 452–464. https://doi.org/10.1016/j.jbusres.2021.07.059
11. Dhar, R. (1997). Consumer preference for a no-choice option. Journal of Consumer Research, 24(2), 215–231. https://doi.org/10.1086/209495
12. Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. Journal of Consumer Research, 21(1), 119–134. https://doi.org/10.1086/209386
13. Efendioğlu, İ. H. (2024). Digital consumer behaviour: A systematic literature review. Psicologia: Reflexão e Crítica, 8(1), 479. https://doi.org/10.32936/pssj.v8i1.479
14. Evans, J. St. B. T. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. Annual Review of Psychology, 59, 255–278. https://doi.org/10.1146/annurev.psych.59.103006.093629
15. Fiore, A. M., Lee, S. H., & Kunz, G. I. (2020). Risk response strategies in high-uncertainty retail contexts. Journal of Retailing, 96(2), 190–205.
16. Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x
17. Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90. https://doi.org/10.2307/30036519
18. Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic decision making. Annual Review of Psychology, 62, 451–482. https://doi.org/10.1146/annurev-psych-120709-145346
19. Gigerenzer, G., Reb, J., & Luan, S. (2022). Smart heuristics for individuals, teams, and organisations. Annual Review of Organisational Psychology and Organisational Behaviour, 9, 171–198. https://doi.org/10.1146/annurev-orgpsych-012420-090506
20. Grass, D., Sonderegger, A., & Sauer, J. (2023). Fast vs. deliberate: Consumers' dual-process decisions in digital product choice. Journal of Consumer Behaviour, 22(4), 345–362. https://doi.org/10.1002/cb.2052
21. Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. Heliyon, e29714. https://doi.org/10.1016/j.heliyon.2024.e29714
22. Hsu, C.-L., & Lin, J. C.-C. (2021). Effects of

perceived value and trust on continuance intention in mobile service usage. Journal of Retailing and Consumer Services, 59, 102393. https://doi.org/10.1016/j.jretconser.2020.102393
23. Huang, T.-L., & Zhang, Z. (2024). Decision-making patterns in digital commerce environments under cognitive load. Electronic Commerce Research and Applications, 56, 102482.
24. Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.
25. Kahneman, D., & Frederick, S. (2002). Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin, & D. Kahneman (Eds.), Heuristics and biases: The psychology of intuitive judgment (pp. 49–81). Cambridge University Press.
26. Kim, D. J., Ferrin, D. L., & Rao, H. R. (2021). A trust-based consumer decision model for online environments. Decision Support Systems, 143, 113495.
27. Kouchaki, M., & Desai, S. D. (2020). Emotions and risk avoidance in consumer decisions. Journal of Consumer Psychology, 30(3), 467–482. https://doi.org/10.1002/jcpy.1207
28. Laato, S., Islam, A. N., Farooq, A., & Dhir, A. (2020). Unusual purchasing behaviour during early stages of the COVID-19 pandemic: The role of perceived threat. Journal of Retailing and Consumer Services, 57, 102224. https://doi.org/10.1016/j.jretconser.2020.102224
29. Lee, M.-C., & Lee, G.-G. (2023). Trust transfer and risk perception in mobile payment adoption. Journal of Financial Services Marketing, 28(4), 227–238.
30. Loewenstein, G. F., Weber, E. U., Hsee, C. K., & Welch, N. (2001). Risk as feelings. Psychological Bulletin, 127(2), 267–286. https://doi.org/10.1037/0033-2909.127.2.267
31. Luce, M. F. (1998). Choosing to avoid: Coping with negatively emotion-laden consumer decisions. Journal of Consumer Research, 24(4), 409–433. https://doi.org/10.1086/209518
32. Mandler, J. M. (2020). Heuristic processing and choice under cognitive stress. Journal of Experimental Psychology: General, 149(6), 1175–1193. https://doi.org/10.1037/xge0000758
33. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81
34. Mitchell, V.-W. (1999). Consumer perceived risk: Conceptualisations and models. European Journal of Marketing, 33(1/2), 163–195. https://doi.org/10.1108/03090569910249229
35. Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. Journal of Marketing, 58(3), 20–38. https://doi.org/10.1177/002224299405800302
36. Park, J., & Lee, E.-J. (2021). Cognitive load and online decision heuristics: Empirical evidence from complex web environments. Computers in Human Behaviour, 120, 106789.
37. Payne, J. W. (1976). Task complexity and contingent processing in decision making: An information search and protocol analysis. Organisational Behaviour and Human Performance, 16(2), 366–387.
38. Payne, J. W., Bettman, J. R., & Johnson, E. J. (1993). The adaptive decision maker. Cambridge University Press.
39. Ravaja, N., Kuppens, P., & Scherer, K. R. (2020). The neurobiological basis of risk and reward in decision making. Journal of Consumer Psychology, 30(3), 560–565.
40. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
41. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social psychophysiology (pp. 153–176). Guilford Press.
42. Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. Academy of Management Review, 23(3), 393–404. https://doi.org/10.5465/amr.1998.926617
43. Schmitt, B. (2024). Consumer information processing and decision-making: Origins, findings, applications, and future directions. Journal of Consumer Research, 51(1), 2–6. https://doi.org/10.1093/jcr/ucae008
44. Sharma, P., Ueno, A., Dennis, C., & Paydas Turan, C. (2023). Emerging digital technologies and consumer decision-making in retail sector: Toward an integrative conceptual framework. Computers in Human Behaviour, 148, 107913. https://doi.org/10.1016/j.chb.2023.107913
45. Sheth, J. (2021). Impact of Covid-19 on consumer behaviour: Will the old habits return or die? Journal of Business Research, 117, 280–283. https://doi.org/10.1016/j.jbusres.2020.05.059
46. Shen, C., & Khalifa, M. (2020). User trust and security perception in digital platforms. International Journal of Human–Computer Studies, 142, 102468. https://doi.org/10.1016/j.ijhcs.2020.102468
47. Slovic, P. (1987). Perception of risk. Science, 236(4799), 280–285. https://doi.org/10.1126/science.3563507
48. Slovic, P., Finucane, M., Peters, E., & MacGregor, D. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. Risk Analysis, 24(2), 311–322. https://doi.org/10.1111/j.0272-4332.2004.00433.x
49. Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? Behavioural and Brain Sciences, 23(5), 645–665. https://doi.org/10.1017/S0140525X00003435
50. Stone, R. N., & Grønhaug, K. (1993). Perceived risk: Further considerations for the marketing discipline. European Journal of Marketing, 27(3), 39–50.
51. Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. Cognitive Science, 12(2), 257–285. https://doi.org/10.1207/s15516709cog1202_4
52. Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

53. Wang, C., & Wang, X. (2022). Digital personalisation and consumer decision consistency. Journal of Interactive Marketing, 59, 69–87.
54. Wang, Y., Yu, C., & Foutz, N. Z. (2023). Consumer fear, uncertainty, and coping strategies in digital marketplaces. Journal of Consumer Marketing, 40(2), 121–135.
55. Zhao, M., & Bacao, F. (2021). What factors determine customer continuance intention in social commerce? Information & Management, 58(3), 103428.
.