



# Information behaviour of data breach victims and the relevance of health information avoidance

Hung Fai Joseph Cheng, Paul Scifleet, and Misita Anwar

DOI: <https://doi.org/10.47989/ir31ISIC65144>

## Abstract

**Introduction.** This study conducts a scoping review and comparative analysis of human information behaviour following data breaches, with a focus on information avoidance. Drawing on parallels with health information behaviour, the research explores how the psychological repercussions of data breaches are shaping cybersecurity victimhood and behavioural responses to digital information post-incident.

**Method.** An interpretive, scoping review methodology is employed to map literature across cybersecurity and health domains. Sources were identified through systematic searches of academic databases, focusing on conceptual overlaps between data breach victimisation and health-related information avoidance.

**Analysis.** Comparative thematic analysis was conducted to identify shared psychological and behavioural traits. Key dimensions included emotional distress, cognitive dissonance, institutional distrust, and uncertainty management. Analysis is synthesised into tables to highlight conceptual convergence.

**Results.** The findings reveal significant parallels between data breach victims and people avoiding health information. Both groups exhibit avoidance driven by anxiety, perceived threats, lack of control, and distrust. Psychological repercussions manifest as digital disengagement, selective exposure, and changes in information behaviour.

**Conclusion.** Information avoidance among data breach victims reflects a complex interplay of emotional, cognitive, and social factors. Understanding these mechanisms is essential for designing supportive interventions and extending health information behaviour theory into the cybersecurity domain.

## Introduction

In an increasingly interconnected digital landscape, the frequency and scale of cybersecurity incidents, particularly data breaches, are emerging as critical risks with far-reaching consequences for people affected by them as they seek to protect themselves and their information from harm online. In the United States, the Federal Bureau of Investigation's Internet Crime Complaint Center recorded 3,204 data breaches and reported losses totalling USD 364,855,818 in 2024 (Internet Crime Complaint Center, 2024). These incidents go beyond technical failures and result in significant life-altering human consequences including psychological trauma, physical health issues, social disruption, and economic hardship.

## Research gap

While research has examined the psychological impacts of cybercrime, little is known about how these experiences shape victims' information behaviours. Existing literature provides limited empirical insight into the ways cybersecurity incidents, particularly data breaches, influence how individuals seek, process, and avoid information. Without this foundational understanding, authorities and organisations lack effective strategies to respond to patterns of information engagement resulting from victimisation. Moreover, it is important to distinguish between public notions of 'victimisation' (e.g., a hacked account) and victims' subjective experiences – how individuals interpret, internalise, and respond to critical incidents. Specifically, there is a notable gap in understanding the information behaviours victims of a data breach adopt: do they modify their online exposure or withdraw from online activities altogether in order to prevent further harm?

## Aim of this paper

This study reviews research on the psychological impacts of data breaches, with a focus on how they shape victims' information behaviours, particularly tendencies toward information avoidance. The extant literature is limited and primarily drawn from psychology and computer science. Although prior studies have examined victims' responses to data breaches (Ayaburi, 2023; Mayer et al., 2023; Mayer et al., 2021; Zou et al., 2018), research explicitly addressing information avoidance remains limited. This study seeks to fill that gap by focusing on victims' tendencies to avoid information following breach incidents. To address this, the study draws from comparative insights from human information behaviour and presents the findings from a scoping review (Howell & Shepperd, 2012; Miller & Mangan, 1983), addressing the following research questions:

RQ1. How can the phenomenon of cybersecurity victimhood be conceptualised to better understand the psychological impacts on individuals and their subsequent information behaviours?

RQ2. What parallels exist between information avoidance and related behaviours in the context of cybersecurity victimisation and established findings from health-related human information behaviour research?

RQ3. How can insights from health-related human information behaviour and information avoidance research inform a preliminary mapping of the psychological impacts of cybersecurity incidents on information behaviours, thereby providing a foundation for future studies in this domain?

## Significance of the study

This research addresses a critical need within cybersecurity response and restitution programs, for understanding how human information behaviour changes as a result of a data breach and the extent to which responses may be intentional or unintentional and result from psychological and social harm. Understanding this behaviour is crucial for developing effective support mechanisms, including access to information services for victims of cybercrime.

By drawing on established health related human information behaviour research, particularly information avoidance and selective exposure (Fischer et al., 2005), this study brings valuable insights to cybersecurity where such understanding is scarce. This interdisciplinary approach will highlight the necessity of expanding understanding of information avoidance and selective information exposure to other domains.

## Research design

### Research methodology

This research employs a qualitative, interpretivist approach to scoping and evaluating current research on changing information behaviours among data breach victims, with a focus on information avoidance and comparing this with human information behaviour research in health contexts. This enables a comparative analysis of concepts, gaps, and parallels between responses to data breaches and health information.

### Research process

The approach taken follows five key steps adapted from Arksey and O'Malley (2005) for scoping literature reviews:

1. *Identifying the research question:* Questions are defined around conceptualising cybersecurity victimhood, exploring parallels with health-related human information behaviour, and applying information avoidance insights to cybersecurity contexts.
2. *Establishing research context:* This step summarises key human information behaviour and information avoidance literature, to provide a foundation for the research, with core concepts of human information behaviour, information avoidance, and cybersecurity, situating the study within its theoretical and empirical context.
3. *Identifying relevant studies for comparative analysis:* This involved a comprehensive search of electronic databases, including Scopus, Google Scholar, ProQuest, EBSCOhost, and reference lists. Keywords for *data breach(es)*, *cybersecurity*, *cybersecurity victim*, *victimisation*, *victimhood*, *information behaviour*, *information avoidance*, *selective exposure*, *health*, *health information* and *psychology* were combined using Boolean operators and targeted filters for precision.

The review covers English-language sources from 2015 to 2025 to show contemporary perspectives on cybersecurity. Eligible sources included peer-reviewed journal articles, conference and symposium proceedings papers, and book sections, resulting in an initial set of 554 articles.

4. *Study selection:* Studies were selected by applying inclusion and exclusion criteria. Titles and abstracts were first screened to exclude irrelevant works; this was followed by a full-text review of remaining articles to confirm eligibility and relevance to the research aims. 90 papers closely aligned with the research focus were identified and selected for comparative analysis in Sections 5 and 6.
5. *Charting analysis and findings:* This step involves systematically extracting, collating, and analysing key findings on human information behaviour and information avoidance to identify conceptual parallels in health and cybersecurity contexts. Analysis is presented through tables and narrative summaries, highlighting similarities, patterns, and gaps to inform comparative analysis and guide future research directions.

## Research context

### Victims of cybercrime

As government and organisations extend digital services, personal information is increasingly exchanged online (Whitson & Davis, 2001). It is an information environment that involves both the push and pull dynamics of personal information required for products and services exchange. It is the rapid, loosely regulated accumulation of personally identifiable information across these channels that has intensified cybersecurity risks (Zaeifi et al., 2024). As vast amounts of client data are collected and disseminated without sufficient safeguards, the number of cybersecurity incidents and data breaches continue to rise, ultimately affecting individuals.

### The rise of cybersecurity incidents

The threat landscape includes malware, online fraud, and identity crimes (Voce & Morgan, 2023). However, data breaches, defined as the unauthorised access or disclosure of personal information (OAIC, 2025a), represent the most critical issue people face in scale and impact (Khan et al., 2022). The Australian *Notifiable Data Breaches Report: July to December 2024* (OAIC, 2025b) recorded 595 breaches, a 15% increase from the previous six months. High-profile breaches included Optus, a major Australian telecommunications provider (2022), which affected 10 million customers; Medibank, Australian health insurance provider (2022), which impacted 9.7 million customers; and Qantas, a flagship airline (2025), comprising 6 million customers. Collectively, these incidents exposed the personal information of tens of millions of Australians, underscoring the far-reaching consequences for victims.

### The impacts of data breaches

Data breaches violate privacy and trust (Kamkar & Duquette, 2021), frequently leading individuals to reassess their digital engagement. Victims experience anxiety, shame, depressive symptoms, and diminished self-esteem (Cross et al., 2016; Kaakinen, 2018), with these psychological effects extending offline and contributing to social withdrawal and isolation (Barnett et al., 1996; Palassis et al., 2021).

Research indicates that cyberattacks can evoke psychological responses comparable to those triggered by terrorism and political violence, with implications for both societal cohesion and individual trauma (Shandler et al., 2023). This threat environment is further exacerbated by perpetrator anonymity, which amplifies risk perception, intensifies anxiety, and discourages victims from using online resources (Cheng et al., 2020; Kaminska & Duquette, 2021).

The rise of cybercrime highlights the need to understand victims' behavioural adaptations. While anxiety (Bada & Nurse, 2019) and withdrawal (Riek et al., 2016) are documented, less is known about proactive coping strategies like selective information exposure or intentional disengagement (Wang, 2024). Furthermore, responses have prioritised organisations over individuals. Muzatko and Bansal (2024) call for research into how victims navigate digital environments post-breach, including decisions to limit online engagement.

### Human information behaviour

Human information behaviour encompasses how individuals seek, process, use, and interact with information, including the influences of cognitive, emotional, social, and situational factors (Spink & Cole, 2004). It encompasses both active information seeking and passive reception, and the routines and practices people develop to engage with information (Savolainen, 2017). Dervin and Nilan (1986) emphasise the individual's active role in shaping information needs through meaning-making, arguing that this process stems from a cognitive drive to create order and coherence from stimuli and thereby enabling greater control and purpose. In this study, information is any distinct signal or source that informs fundamentally influencing behaviour, thought, decision-making, emotion, and social interaction (Case et al., 2023; Velmans, 1991).

Information needs arise not only during problem-solving scenarios, like health diagnoses, which create immediate needs to understand situations and outcomes (Case et al., 2023), but also from curiosity, social connection, or entertainment. From a cognitive perspective, internal knowledge structures are continually updated, and any situation where existing mental models are insufficient, due to complex problems or simple curiosity, drive the resolve to adjust (Belkin, 1990). In today's digital environment, a shift from scarcity to overabundance has transformed engagement, creating risks of overload and disengagement. Faced with excessive or conflicting information, some users may disengage entirely, a phenomenon coined as information avoidance in human information behaviour research (Sweeny et al., 2010), and closely linked to selective exposure to information (Fischer et al., 2005).

### Information avoidance

With online engagement, increasing numbers of researchers have highlighted the growing relevance of information avoidance, including its role in responses to public health messaging during health crises (Huvila & Gorichanaz, 2025). Information avoidance, defined as 'any behaviour intended to prevent or delay the acquisition of available but potentially unwanted information' (Sweeny et al., 2010), encompasses evading sources, withdrawing from disclosure environments, or ignoring cues. Initially conceptualised as a psychological defence mechanism against anxiety (Sweeny et al., 2010), it aligns with cybersecurity victims' behaviour, especially when considered as a strategic response to the impacts of data breach. Qi et al. (2024) further framed it as a deliberate behavioural strategy where individuals weigh emotional strain, risks, and costs against perceived benefits, reflecting a shift from viewing avoidance as unconscious protection to an intentional decision.

Selective exposure is closely associated with information avoidance and has been extensively studied through psychological and cognitive behavioural lenses (Hart et al., 2009; Sweeny et al., 2010). Research shows that individuals often seek information that confirms existing beliefs while avoiding contradictory content (Neal et al., 2024; Nickerson, 1998), and can be driven by anxiety, fear, self-efficacy, and locus of control (Case et al., 2005; Foust & Taber, 2024; Golman et al., 2017). Several studies have examined cognitive dissonance, emphasising that individuals tend to avoid information that challenges their existing beliefs and self-perceptions (Miller & Mangan, 1983; Narayan et al., 2011; Sultana et al., 2023).

Contemporary perspectives recognise selective exposure as a nuanced manifestation of information avoidance that encompasses both selection and avoidance behaviours (Case et al., 2023). Building on this, Hicks et al. (2024) framed avoidance as practices that moderate information engagement by reducing intensity, limiting control, or filtering content, emphasising that avoidance is not inherently maladaptive but a complex, potentially beneficial information practice (Hicks et al., 2024; Smith et al., 2008; Sweeny et al., 2010).

Research on information behaviour and avoidance has been applied across diverse disciplines, including health sciences (Davies & Harrison, 2007), business (Auster & Choo, 1993), law (Sutton, 1994), psychology (Lévai et al., 2024), and communication studies (Agarwal et al., 2022), reflecting growing interdisciplinary engagement (Agarwal, 2023; Foust et al., 2023). Cybersecurity, which is now central to individuals, organisations, and national security (Hytönen et al., 2022; Schiliro, 2023), provides a critical context for extending this field.

### Charting identity in data breach narratives

Victim, survivor, affected individual, or data subject?

The terminology used to describe individuals affected by data breaches varies and includes *victim*, *affected individual*, *survivor*, and *data subject*. Constructing identity through the vocabulary used in data breach narratives is crucial as it shapes societal perceptions, legal responses, and individual

agency. Each term carries substantive implications for psychological wellbeing and legal standing following breach events.

The term *victim* emphasises harm and liability and invokes sympathy (Golladay & Holtfreter, 2016). The term *survivor* shifts focus to resilience and empowers affected individuals while highlighting systemic failures in data governance (Hurtado et al., 2021). *Affected individual* acknowledges harm without subjectivity, while *data subject* rooted in legal frameworks like the General Data Protection Regulation (GDPR) diminishes personal trauma (GDPR, 2016).

### Terminology framing individuals affected by data breaches

*Victim* remains the dominant term across academia, government, and media. A July 2025 PressReader search for *data breach* AND *victim* yielded 1,990 English-language media articles from the prior year. In contrast, *data breach* AND *survivor* returned 150 articles, over 90% of which referenced unrelated contexts (e.g., domestic violence) in PressReader. *Affected individual* appeared in only seven articles (two incident-related), while *data subject* appeared 41 times, primarily in legislative discourse.

The term *victim* underscores harm and vulnerability (Golladay & Holtfreter, 2016), consistent with dictionary definitions, whereas *survivor* connotes resilience and proactive risk management (Hurtado et al., 2021). Legal frameworks typically favour neutral terms such as *affected individual* or *data subject* (e.g., Office of the Privacy Commissioner of Canada, HIPAA, NIST).

In psychological contexts, adopting *survivor* terminology fosters empowerment and control, and this seems particularly relevant to cybersecurity incidents that may induce trauma (Delker et al., 2019), as it gives shape to coping strategies. While *victim* may reinforce helplessness, *survivor* encourages positive, protective behaviours (Van Dijk, 2020; Delker et al., 2020), that may extend to include processing breach information, safeguarding digital assets, and recalibrating trust in digital systems.

| Jurisdiction          | Legal framework                                                       | Terminology used             | Rationale/approach                                                                              |
|-----------------------|-----------------------------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------|
| European Union (2016) | General Data Protection Regulation (GDPR)                             | Data subject                 | Neutral; emphasising legal standing and agency rather than victimhood                           |
| United States         | Consumer protection Laws (Legal Information Institute, 2025)          | Affected consumer / Resident | Reflects consumer protection framework while avoiding presumption of harm that 'victim' implies |
| United Kingdom        | EU GDPR (2016) / Data Protection Act (2018)                           | Data subject                 | Maintains consistency with EU approach, emphasising legal standing rather than victimhood       |
| Canada (2018)         | Personal Information Protection and Electronic Documents Act (PIPEDA) | Affected individual          | Acknowledges impact without presuming degree of harm                                            |
| Australia (2018)      | Privacy Act / Notifiable Data Breaches scheme                         | Affected individual          | Acknowledges impact without presuming degree of harm                                            |
| New Zealand (2020)    | Privacy Act                                                           | Affected individual          | Acknowledges impact without presuming degree of harm                                            |

|                  |                                     |            |                                                                     |
|------------------|-------------------------------------|------------|---------------------------------------------------------------------|
| Japan (2022)     | Personal Information Protection Act | Principal  | Formal; emphasising individual's primary relationship to their data |
| Singapore (2012) | Personal Data Protection Act        | Individual | Neutral term avoiding any presumption about impact or harm          |

**Table 1:** Terminology used in different jurisdictions.

Table 1 illustrates how variations in terminology across jurisdictions and data protection laws reflect legal frameworks governing individual rights and corporate responsibilities. Terms like *affected individual* or *data subject* assign a clear legal status without presupposing harm and distinguish individuals from corporations in the context of cyberattacks (Bygrave, 2020; Mantelero, 2018; Sargiotis, 2024).

While companies are responsible for safeguarding data and may suffer financial or reputational harm when a breach occurs, individuals' rights to data protection and recourse are legally established in these contexts (Schwartz & Peifer, 2017; Solove & Citron, 2017). However, the recourse available is often procedural and lengthy. In Australia, it typically requires first seeking a response directly from the company whose security failed; if unresolved, the matter proceeds to the Office of the Australian Information Commissioner for investigation and may culminate in legal action involving other areas of law, like Australian Consumer Law.

Neutral terminology risks shifting the burden of proof onto individuals, who must demonstrate harm, like emotional distress, to pursue legal recourse. By adopting neutral language, legal discourse directs attention to existing legal rights and organisational accountability, but does not acknowledge the affective dimensions of suffering. This tendency aligns with broader societal shifts favouring *survivor* narratives that emphasise resilience and active coping (Herman, 2015). Although legal frameworks rarely use the term *survivor* explicitly, such terms frame victims as empowered actors, aligning with human information behaviour research that views selective information exposure as a deliberate strategic response (Hicks et al., 2024).

A literature search across academic databases reveals notable differences in terminology describing individuals affected by data breaches. Searches were conducted in ProQuest, Scopus, and ten Tier-1 cybersecurity journals, which are highly ranked publications recognised for rigorous peer review, high impact factors, and strong influence on scholarly discourse. The results, summarised in Tables 2 and 3, reflect usage patterns across key terms (Criteria: Published 2015–2025; Language: English; Full-text only). Table 2 presents term frequencies in academic databases, while Table 3 shows terminology prevalence in Tier-1 journals.

| Key terms                               | ProQuest | Scopus |
|-----------------------------------------|----------|--------|
| 'Data Breach' and 'Victim'              | 309      | 1,093  |
| 'Data Breach' and 'Survivor'            | 1        | 83     |
| 'Data Breach' and 'Affected Individual' | 3        | 24     |
| 'Data Breach' and 'Data Subject'        | 3        | 213    |

**Table 2:** Key terms used in academic databases.

| Journal                                                 | Survivor | Data subject | Affected individual | Victim     |
|---------------------------------------------------------|----------|--------------|---------------------|------------|
| IEEE Transactions on Dependable and Secure Computing    | 0        | 25           | 0                   | 3          |
| IEEE Transactions on Information Forensics and Security | 0        | 1            | 0                   | 1          |
| Journal of Cybersecurity                                | 0        | 6            | 6                   | 1          |
| IEEE Security and Privacy                               | 0        | 3            | 0                   | 21         |
| IET Information Security                                | 0        | 0            | 0                   | 0          |
| ACM Transactions on Privacy and Security                | 0        | 1            | 0                   | 8          |
| Journal of Cryptology                                   | 3        | 45           | 1                   | 67         |
| Cryptologia                                             | 1        | 17           | 0                   | 0          |
| Computer Law & Security Review                          | 0        | 0            | 27                  | 60         |
| ACM Transactions on Computer Systems                    | 0        | 3            | 0                   | 102        |
| <b>Total number of usages</b>                           | <b>4</b> | <b>101</b>   | <b>34</b>           | <b>263</b> |

**Table 3:** Key terms used in 10 Tier-1 journals on computing and cybersecurity.

The term *victim* features prominently in academic databases and journals (ProQuest: 309; Scopus: 1,093), reflecting a persistent framing of data breaches as events causing definitive harm. This reinforces narratives of victimisation and human cost (Golladay & Holtfreter, 2016; Hay & Ray, 2019; Kilovaty, 2021), and from a social and psychological perspective, the label risks stigmatisation and secondary harm by implying passivity, contradicting empowerment-focused recovery approaches (Delker, 2022). Furthermore, since not all victims experience tangible negative outcomes or self-identify with the term, its use can misalign with lived experience (Budimir et al., 2021).

### How data breach terminology shapes understanding of victimhood

The variation in terminology varies across context: public and academic discourse often use *victim* to acknowledge harm, while legal terms like *data subject* or *affected individual* aim to avoid assumptions about harm severity (Solove & Citron, 2016). *Survivor* implies response and recovery and, while empowering, it may not reflect the initial state of those impacted, particularly when many lack resources to respond effectively.

This research adopts *victim* to emphasise violations of autonomy, privacy, and security, while distinguishing between victimisation (a harmful event), and victimhood (the defining social, psychological and discursive frame). By focusing on individuals affected by data breaches, the term *victim* allows this study to centre on the lived experience of people rather than organisations. Unlike companies, which can draw on institutional resources, individual recourse is often slow and uncertain.

Understanding the impacts of a data breach through the lenses of *affected individuals*, *data subjects*, and *survivors* is an important part of victimhood. However, this study prioritises the human impact, acknowledging the psychological, social, and practical consequences experienced by individuals whose personal information has been compromised. This perspective recognises the agency, power, and strategic choices that data breach victims exercise through their information practices.

## Distinctive traits of data breach victims

Cybersecurity and psychology research highlights changed behaviours among data breach victims, driven by psychological traits that extend beyond financial and technical harm. Victims often experience prolonged emotional distress, including anxiety, vulnerability, and institutional distrust, especially when breaches involve sensitive personal or health-related information. These are compounded by uncertainty surrounding delayed identity misuse and poor institutional support (Sears & Cunningham, 2024; Cross & Holt, 2025). Yet, these behaviours remain underexplored within the framework of human information behaviour. This section addresses that gap by identifying key psychological traits, like anxiety, distrust, and vulnerability, and mapping them to corresponding information avoidance behaviours.

## The psychological repercussions of data breaches

Data breaches have profound psychological tolls on individuals, extending beyond financial loss to a sustained erosion of trust and autonomy, cognitive overload, and feelings of helplessness (Kilovaty, 2021; Sears & Cunningham, 2024). The breach of institutional trust constitutes a distinct harm, as victims confront material consequences including violations of personal privacy. Research indicates that the anxiety experienced is not fleeting, but a persistent psychological response to perceived loss of control over one's data and life (Bada & Nurse, 2019; Nurse, 2018). Despite remediation mechanisms, organisational and regulatory frameworks frequently neglect the emotional aftermath, leaving victims unsupported.

Unlike other cybercrimes, the enduring ambiguity that data breaches generate regarding the scope of exposure and potential misuse of information causes stress, hypervigilance, and a cycle of psychological distress (Jansen & Leukfeldt, 2018; Palassis et al., 2021; Sears & Cunningham, 2024). PTSD-like symptoms include intrusive thoughts, emotional withdrawal, and avoidance behaviours, such as avoiding information about a breach or the digital service that was breached (Pfleeger & Caputo, 2012; Rhoads, 2023). Information avoidance, while protective, may also signal deeper trauma, underscoring the need for institutional responses informed by shifts in human information behaviour. Unlike physical theft, digital breaches lack clear recovery pathways, exacerbating helplessness and disempowerment.

The Medibank Private Health Insurance breach in Australia exemplifies the heightened psychological impact of compromised health information, where fear of public disclosure triggered shame, anxiety, and vulnerability (Rhoads, 2023). The central concern remains the persistent uncertainty surrounding future exploitation of compromised data. Responses to breaches vary, shaped by factors like financial loss, data sensitivity, and institutional inaction. Emotional distress, while a recognised mediator between harm and coping, risks oversimplifying the complexity of victims' experiences (Li et al., 2019). Moreover, inadequate support structures compound helplessness and hinder recovery (Koch & Adeleye, 2019).

Nobles (2022) describes 'risky disengagement' as a response to cognitive and emotional strain, wherein individuals overwhelmed by alerts and protocols withdraw from safe practices. Cognitive overload impairs decision-making, as mental fatigue undermines vigilance. Recovery is often protracted and burdensome, involving account monitoring, credential changes, and institutional engagement. These efforts, perceived as disproportionate to uncertain benefits, may foster futility and disengagement (Bryant, 2025). Over time, victims may ignore future warnings or change online patterns to reduce exposure (Kirlappos et al., 2013; Stanton et al., 2016).

## Behavioural adaptations in the aftermath of data breaches

This research frames information avoidance following data breaches not as anomalous, but as an emotional and behavioural response to a perceived threat, loss of control, and trauma. Evidence shows such reactions often lead to digital withdrawal as a psychological response (Barbour et al.,

2012; Hayes et al., 1996; Hoffmann et al., 2016). Information avoidance may include reduced online activity, reluctance to engage with compromised services, or complete disengagement.

LaRose et al., (2008) proposes that individuals who perceive a threat as severe but feel incapable of responding effectively are more likely to disengage than take constructive action. This response, rooted in low self-efficacy and heightened vulnerability, can extend to denial, deferment, and emotional withdrawal (LaRose et al., 2008; see also Chu & Liu, 2023). Recent findings support this perspective. Verizon (2023) found that individuals often ignore security alerts due to low confidence in their ability to respond, and such disengagement reflects an adaptive strategy for reducing cognitive and emotional strain rather than irrational behaviour (Barbour et al., 2012; Hicks, 2024; Liu, 2022).

Information avoidance serves as a coping mechanism to ease emotional strain, ranging from temporary retreat to sustained disengagement (Hicks et al., 2024; Liu & Chen, 2024; Park et al., 2024; Riek et al., 2016). For example, Brashers (2001) found that individuals awaiting genetic test results often postpone accessing the report or avoid discussions to manage distress, preserve equilibrium, and maintain a sense of control amid uncertainty. Table 4 synthesises these findings and provides a foundation for the following section, which draws on health information avoidance research to establish a comparative framework for theorising the information behaviours of data breach victims.

| Category                    | Characteristic                                              | Description                                                                                                                                                                | Reference                                                                                                  |
|-----------------------------|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Psychological repercussions | Psychological distress; Anxiety                             | Persistent worry, emotional turmoil, and agitation following a data breach, may intensify with sensitivity of exposed data.                                                | Bada & Nurse (2019); Nurse (2018); Jansen & Leukfeldt (2018)                                               |
|                             | Violation of privacy and autonomy                           | Sense of boundary infringement and powerlessness, eroding self-efficacy; May correlate with financial loss, data misuse, and resolution time, mediating coping behaviours. | Palassis et al., (2021); Sears & Cunningham (2024); Li et al. (2019); Stanton et al. (2016); Bryant (2025) |
|                             | Helplessness; Loss of control; Loss of confidence           | Victims feel powerless due to lack of involvement in the breach and limited ability to prevent future harm.                                                                | Palassis et al. (2021); Sears & Cunningham (2024); Jansen & Leukfeldt (2018)                               |
|                             | Victimisation severity                                      | Distress influenced by extent of financial loss, data misuse, and resolution time, mediating coping behaviours.                                                            | Li et al. (2019)                                                                                           |
|                             | Persistent uncertainty; Heightened vulnerability            | Ongoing ambiguity about data exposure and use, leading to amplified perceptions of risk.                                                                                   | Sears & Cunningham (2024); Jansen & Leukfeldt (2018)                                                       |
|                             | Chronic stress; Hypervigilance; Hyperarousal; Fatigue       | Long-term activation of stress response system, marked by sustained alertness, physiological tension, and exhaustion.                                                      | Jansen & Leukfeldt (2018); Palassis et al. (2021); Nobles (2022)                                           |
|                             | Cognitive overload; Intrusive thoughts; Negative cognitions | Mental exhaustion from constant security demands, recurrent involuntary breach-related thoughts, and pessimistic beliefs.                                                  | Nobles (2022); Jansen & Leukfeldt (2018); Sears & Cunningham (2024)                                        |
|                             | Trauma; Fear; PTSD                                          | Deep distress and intense apprehension, may be triggered by exposure of highly sensitive personal information; and post-trauma stress                                      | Golladay and Holtfreter (2016); Pfleeger (2012) and Rhoads (2023)                                          |

| Category             | Characteristic                                                     | Description                                                                                                                                                                    | Reference                                                                     |
|----------------------|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
|                      |                                                                    | disorder (PTSD) developed after experiencing a data breach.                                                                                                                    |                                                                               |
| Behavioural Response | Changing online engagement                                         | A continuum of avoidance that can range from minor changes in online habits (e.g., selectively securing accounts) to complete disengagement from digital life.                 | Hayes et al. (1996); Barbour et al. (2012); Riek et al. (2016)                |
|                      | Abandoning not adopting safeguards                                 | Distrust and low self-efficacy are associated with reduced trust and confidence in managing threats, leading users to abandon platforms rather than adopt protective measures. | Hoffmann et al. (2016); LaRose et al. (2008)                                  |
|                      | Ignoring breach notifications and security alerts                  | Driven by feelings of helplessness or low self-efficacy, individuals may ignore warnings about breaches or security alerts, as they feel incapable of responding effectively.  | Verizon DBIR (2023)                                                           |
|                      | Selective information filtering                                    | To manage emotional distress, individuals may actively filter or avoid threat-related information and news about data breaches.                                                | Brashers (2001); Barbour et al. (2012)                                        |
|                      | Excessive monitoring of accounts or devices                        | Ongoing account monitoring due to fear of re-victimisation, leading to heightened anxiety and reduced quality of life.                                                         | Jansen & Leukfeldt (2018)                                                     |
|                      | PTSD responses - withdrawal, hyperarousal, and negative cognitions | PTSD symptoms include intrusive thoughts, digital withdrawal, hyperarousal, and negative cognitions developed after prolonged exposure to uncertainty and perceived threat.    | Mateu et al. (2020); Pfleeger (2012); Pfleeger & Caputo (2012); Rhoads (2023) |

**Table 4:** Summary of psychological repercussions and behavioural responses to data breaches

## The prevalence and drivers of health information avoidance

This section reviews the prevalence and underlying drivers of health information avoidance as human information behaviour that are both widespread and nuanced. The research shows that, although the frequency and causes vary across populations and health issues (Barbour et al., 2012; Melnyk & Shepperd, 2012), avoidance is not incidental. Rather, it reflects a complex interplay of psychological, cognitive, and social mechanisms which shape how individuals engage with health information.

### Psychological drivers of health information avoidance

Health information avoidance is described as driven by emotional distress, cognitive dissonance, and perceived lack of control (Brashers et al., 2002; Case et al., 2005; Melnyk & Shepperd, 2012; Sairanen & Savolainen, 2010). Karlsson et al. (2009) describe this response as the 'ostrich effect', a tendency to avoid threatening situations to reduce anxiety and fear. Emotional distress leads individuals to disengage from information perceived as overwhelming. Similarly, Festinger's (1957) theory of cognitive dissonance offers an explanation of how individuals may reject or ignore health information that conflicts with their personal beliefs, thereby preserving a coherent self-concept. Howell and Shepperd (2012) illustrate this in dietary habits, where individuals dismiss risk-related information to avoid confronting long-term consequences.

Howell and Shepperd (2013) found that perceived powerlessness intensifies information avoidance, transforming it from passive reaction to deliberate coping. This is evident in hereditary conditions like breast cancer, where individuals may avoid learning early symptoms due to low coping capacity or belief in futility (Melnik & Shepperd, 2012). Some responses may be automatic and uncontrolled (Howell et al., 2016).

When coping resources are low, or core beliefs challenged, selective exposure may arise as strategy, such as seeking information that confirms existing beliefs while avoiding threatening information (Fischer et al., 2005; Hart et al., 2009; Tsang, 2017). Brashers et al., (2002) demonstrate how information avoidance can have a collective dimension, as a strategic response enacted by individuals, family members and health care providers as a mechanism for reducing stress.

Cultural and community dynamics further shape avoidance, with stigma and fear of judgment deterring engagement in contexts like mental illness, HIV/AIDS, and substance abuse (Earnshaw & Chaudoir, 2009).

Information overload and source credibility concerns further complicate individuals' willingness to engage with health information (Case et al., 2005; Sweeny et al., 2010). Social networks can thus reinforce or mitigate the effects of avoidance.

### Behavioural adaptation of avoidance in health contexts

Deliberate avoidance of health information is significant, with research showing that 20% of high-risk individuals forego HIV testing (Barbour et al., 2012) and 15–30% of eligible adults delay or skip cancer screenings (Melnik & Shepperd, 2012). It is also evident in everyday behaviours, like ignoring nutritional labels and disengaging from public health campaigns (Howell et al., 2016; Sweeny et al., 2010). Of greatest concern is that it can lead to delays in medical intervention, when early treatment is critical (Taber et al., 2015). During the COVID-19 pandemic, 20.2% of symptomatic individuals actively avoided seeking further information, illustrating the broader public health implications of avoidance because of fear of positive diagnosis and perceived helplessness (Czeisler et al., 2020).

These findings show that health information avoidance is not irrational, but a series of responses shaped by distress, dissonance, lack of control, stigma, or distrust (Brashers et al., 2002; Case et al., 2005). This underpins a spectrum of behaviours, from passive neglect to active disengagement, shaped by factors such as threat severity, social norms, and information saturation. Table 5 applies the analytical framework, by categorising health information avoidance literature in terms of psychological repercussions and behavioural responses associated with information avoidance and presents a model for comparison.

| Category                    | Characteristics               | Description                                                                                                                                      | Reference                                                                                   |
|-----------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Psychological repercussions | Fear; anxiety; distress       | Individuals may avoid health information to escape distress, especially in high-stakes contexts like genetic testing for untreatable conditions. | Karlsson et al. (2009); Taber et al. (2015); Brashers et al. (2000); Brashers et al. (2002) |
|                             | Lack of Control; helplessness | Feeling powerless (e.g., due to genetic predisposition) can lead individuals to avoid information to escape helplessness.                        | Howell et al. (2013); Howell et al. (2016)                                                  |
|                             | Threat Severity               | Distress correlates with serious illness (e.g., cancer, HIV) and avoidance increases with                                                        | Barbour et al. (2012); Melnyk & Shepperd (2012)                                             |

| Category             | Characteristics                                          | Description                                                                                                                                                           | Reference                                                                                  |
|----------------------|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
|                      |                                                          | perceived severity of the health threat.                                                                                                                              |                                                                                            |
|                      | Cognitive overload                                       | Overwhelmed by excessive or complex health information (information overload).                                                                                        | Howell et al. (2016); Sweeny et al. (2010)                                                 |
| Behavioural Response | Stigma, or social norms discouraging information-seeking | Social stigma (e.g., around HIV or mental health) may deter information-seeking due to fear of judgment or exclusion.                                                 | Earnshaw & Chaudoir (2009)                                                                 |
|                      | Distrust in source, perceived inconsistency              | Inconsistent or unreliable messaging (e.g., public health campaigns); Scepticism toward institutions or experts can drive deliberate avoidance of health information. | Sweeny et al. (2010); Brashers et al. (2002); Case et al. (2005)                           |
|                      | Ignore or denying results                                | To preserve optimism, individuals may ignore or deny test results (e.g., skin cancer screenings), preferring uncertainty over confirmed risk.                         | Sweeny et al. (2010); Howell et al. (2016); Brashers et al. (2000); Brashers et al. (2002) |

**Table 5:** Factors of Health Information Avoidance

## Parallel behaviours: Psychological and human information behaviour commonalities between health information avoidance and data breach victimhood

Information avoidance occurs in distinct contexts from coping with data breaches to managing health conditions within human information behaviour. In both, individuals face threats and respond by avoiding or selectively engaging with information. Literature shows that breach victims filter, or reject information that undermines security and control, mirroring human information behaviour findings on health information avoidance, including planned and unconscious avoidance, selective exposure, and disengagement.

### Emotional response

Both areas of research involve individuals responding to significant threats. Data breach victims face prolonged anxiety from identity theft, financial harm, and reputational damage (Bada & Nurse, 2019), exacerbated by uncertainty about future data misuse (Sears & Cunningham, 2024). Similarly, individuals experience distress when confronted with potentially serious or stigmatised diagnoses (Karlsson et al., 2009), leading them to avoid medical tests or limit information as a psychological defence (Taber et al., 2015). In both, avoidance serves to reduce anxiety, but risks long-term impacts.

### Cognitive dissonance

Cognitive dissonance underpins avoidance in both contexts. Data breach victims may ignore security warnings or minimise risks to preserve trust in digital systems (Nobles, 2022), like individuals avoiding medical information that conflicts with their lifestyle choices (Festinger, 1957). In both cases, selective exposure maintains psychological equilibrium by filtering out threatening information. This may manifest as abandoning or limiting online services (Riek et al., 2016), or skipping health screenings and doctor visits (Melnik & Shepperd, 2012).

### Perceived lack of control

Diminished control impacts behaviour in both circumstances. Data breach victims feel powerless due to organisational failures, with limited individual recourse to prevent future harm (Sears & Cunningham, 2024), leading to disengagement (Kirlappos et al., 2013). Similarly, people who avoid health information may believe they cannot change health outcomes (Howell et al., 2013). Research to date indicates that perceived lack of control reinforces the prioritisation of short-term emotional relief over long-term risk management and is presented as a passive coping mechanism.

### Trust violations and institutional distrust

Data breach victims feel betrayed by corporations failing to protect data, fostering digital platform distrust (Muzatko & Bansal, 2024). This mirrors people avoiding health information because negative experiences, conflicting advice, or healthcare scepticism creating institutional mistrust (Brashers et al., 2002). In both cases, the erosion of trust exacerbates avoidance reducing compliance with security protocols or preventive healthcare measures (Brashers et al., 2002).

### Uncertainty management and preference for ambiguity

Uncertainty about outcomes is a significant stressor leading to information avoidance, with individuals preferring 'not to know' over distressing certainty. Data breach victims may avoid checking the status of compromised data to delay confronting risks (Cross et al., 2025), while people experiencing illness may avoid health information to maintain hope (Zhu et al., 2024). This 'motivated ignorance' involves actively avoiding information to manage emotional states, preserving wellbeing despite unpreparedness for future threats.

### Stigma and social consequences

Stigma contributes to avoidance in distinct ways across domains. Data breach victims may withdraw socially due to shame over exposed sensitive information (Rhoads, 2023), while individuals with stigmatised health conditions may avoid medical information to escape judgment or discrimination (Earnshaw & Chaudoir, 2009). Societal perceptions heighten avoidance as individuals weigh the risks of social exposure against the benefits of threat mitigation.

### Long-term consequences of avoidance

Avoidance behaviours compound risks over time. Data breach victims disengaging from security measures become more vulnerable to subsequent attacks (Jansen & Leukfeldt, 2018), while people avoiding health information may face poorer outcomes from delayed diagnosis or treatment (Melnik & Shepperd, 2012). The persistent nature of avoidance, where short-term relief reinforces long-term harm, is often accompanied by chronic stress from unresolved threats.

These parallels between health information avoidance and data breach victimhood are summarised in Table 6, which compares psychological and behavioural characteristics across both domains. The table illustrates how emotional responses, cognitive factors, perceived lack of control, trust violations, uncertainty management, stigma, and long-term consequences manifest similarly in cybersecurity and health contexts.

| Category                    | Characteristics    | Cybersecurity impacts (data breach victims)                                                                       | Health information avoidance                                                                                                       |
|-----------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Psychological repercussions | Emotional response | Fear Anxiety, distress, and trauma due to loss of control and uncertainty about data misuse. (Bada & Nurse, 2019) | Fear, anxiety, distress and trauma triggered by potential health diagnoses or negative health information. (Karlsson et al., 2009) |
|                             | Cognitive factors  | Cognitive overload leads to security fatigue and disengagement. (Nobles, 2022)                                    | Cognitive dissonance leads to avoidance of conflicting health information. (Festinger, 1957)                                       |

| Category             | Characteristics               | Cybersecurity impacts (data breach victims)                                                             | Health information avoidance                                                                                                                                                                                         |
|----------------------|-------------------------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Lack of control, helplessness | Victims feel helpless due to lack of control over breached data. (Sears & Cunningham, 2024)             | Individuals avoid health information if they believe they cannot change outcomes (e.g., genetic risk). (Howell et al., 2013)                                                                                         |
|                      | Uncertainty                   | Persistent uncertainty about how exposed data will be exploited. (Brashers, 2001)                       | Uncertainty surrounding potentially unfavourable outcomes, such as declining genetic testing to evade anxiety about future illness or difficult medical decisions. (Zhu et al., 2024, Sairanen and Savolainen, 2010) |
| Behavioural Response | Trust & betrayal              | Breach of trust in organisations that failed to protect data. (Muzatko & Bansal, 2024)                  | Distrust in medical institutions or conflicting health advice leads to avoidance. (Brashers et al., 2002)                                                                                                            |
|                      | Ignoring, self-selecting      | Withdrawal from digital services, ignoring security alerts. (Barbour et al., 2012)                      | Avoiding screenings, ignoring health warnings, or disengaging from medical information. (Riek et al., 2016)                                                                                                          |
|                      | Stigma & social influence     | Cyber trauma may lead to social withdrawal due to shame (e.g., leaked sensitive data). (Rhoads, 2023)   | Stigma around certain illnesses (e.g., HIV, mental health) discourages information-seeking. (Earnshaw & Chaudoir, 2009)                                                                                              |
|                      | Long-term impact              | Hypervigilance, PTSD-like symptoms, and chronic stress from ongoing threats. (Jansen & Leukfeldt, 2018) | Long-term harm from delayed medical intervention due to avoidance. (Melnik & Shepperd, 2012)                                                                                                                         |

**Table 6:** The similarities between the characteristics of data breach victims and health information avoiders

While threats differ, the psychological and behavioural parallels between data breach victims and people who avoid health information are prominent. Both groups employ information avoidance as a coping mechanism to manage fear, uncertainty, and perceived loss of control.

## Discussion and conclusion

This analysis shows that both data breach victims and individuals avoiding health information exhibit similar coping responses to threatening situations. Both face emotional distress, through identity theft or financial harm in breaches (Bada & Nurse, 2019; Sears & Cunningham, 2024), and individuals who avoid health information, through anxiety about potential serious or stigmatised diagnoses (Karlsson et al., 2009; Taber et al., 2015). In both, information avoidance is a primary coping strategy (Hicks et al., 2024; Sweeny et al., 2010).

The study has addressed three interrelated research questions concerning the conceptualisation of victimhood in cybersecurity (RQ1), the behavioural parallels between information avoidance in data breach contexts and health-related human information behaviour (RQ2), and the applicability of insights from health-related human information behaviour and information avoidance literature to cybersecurity research (RQ3).

In response to RQ1, the findings call for reframing cybersecurity victimhood's legal and technical focus to include human information behaviour and the psychological experiences of affected individuals. *Victim* should be seen as a dynamic identity, shaped by lived experience including

trauma, impact and personal response. This re-conceptualisation facilitates a more empathetic and human-centred lens for people affected by data breaches.

Addressing RQ2, substantial parallels exist between information avoidance in data breach cases and health-related human information behaviour (Brashers et al., 2002; Howell & Shepperd, 2012). In both domains, avoidance is often driven by emotional distress, uncertainty, and a perceived loss of control (Melnyk & Shepperd, 2012; Nobles, 2022). For example, individuals may decline genetic testing to avoid confronting potential diagnoses, just as data breach victims may ignore breach notifications to delay dealing with the consequences of compromised personal data. These adaptive coping strategies reflect shared issues of trust, stigma, and long-term impact, highlighting information avoidance as a cross-contextual phenomenon that can inform cybersecurity responses. Furthermore, the commonalities identified in this review could be extended to other human information behaviour contexts where perceived threat levels and emotional distress are high.

In addressing RQ3, this study applies health-related human information behaviour and information avoidance literature to cybersecurity, highlighting information avoidance as a strategic response to emotional and cognitive overload. The role of stigma and social norms in discouraging information engagement is highly relevant to cybersecurity contexts, where shame and fear of judgment can suppress proactive behaviours (Earnshaw & Chaudoir, 2009; Rhoads, 2023). These insights advocate for a more nuanced and psychologically informed approach to cybersecurity research and organisational responses to data breaches, drawing on information science, health-related information behaviour, behavioural studies, and health communication research to better support individuals affected by data breaches.

## Limitations and future directions

This study acknowledges several limitations. It is limited by a lack of existing literature and research on information behaviour in cybersecurity context and as such, it may not capture the unique nuances of data breach experiences through comparison with health-related information avoidance. At this point in time, it does not involve primary data collection from data breach victims which remains essential for richer, direct insights into their experiences.

To address these limitations, the next stage of research will begin with a questionnaire targeting victims of cybersecurity incidents to collect demographic data and examine changes in information behaviour following a breach. From this respondent pool, qualitative semi-structured interviews will be conducted to capture detailed accounts of psychological impacts, coping strategies, and engagement patterns. Finally, focus groups will be organised with victims to collaboratively develop strategies that support recovery and improve information engagement.

## Implications

The findings of this study provide significant theoretical and practical contributions to information behaviour research within cybersecurity contexts. Theoretically, this work extends human information behaviour and information avoidance frameworks by illustrating how breach victimisation shapes avoidance-oriented behaviours in digital environments. While parallels exist between health-related and cybersecurity contexts, this study acknowledges the distinct experiential and social environments surrounding data breaches and emphasises adapting insights from health information behaviour to these unique conditions. It emphasises the interplay between risk perception, cognitive load, and coping strategies, offering a foundation for future empirical studies and interdisciplinary dialogue between information behaviour and cybersecurity research.

Practically, these insights inform the development of victim-centred interventions that address psychological and behavioural consequences of data breaches. Communication strategies should reduce cognitive complexity and incorporate empathetic messaging to mitigate avoidance and

encourage proactive engagement. Policy and regulatory frameworks can integrate behavioural principles into breach notification requirements, supporting informed decision-making while minimising anxiety and uncertainty. Digital literacy programs should embed human information behaviour constructs, such as self-efficacy and resilience, to counteract disengagement and foster adaptive information practices. Additionally, digital platforms and user interfaces should prioritise simplicity, trust-building, and coping support to enable victims to re-engage with information and recover effectively.

This study also identifies several directions for future research beyond the next stage of data collection. Longitudinal studies could examine how information avoidance evolves over time following breach incidents, capturing changes in coping strategies and engagement patterns. Comparative research across cultural and demographic contexts would deepen understanding of social and psychological factors influencing avoidance behaviours. Integrating human information behaviour and information avoidance frameworks with emerging theories in digital risk communication may yield richer models of decision-making under uncertainty. Finally, interdisciplinary collaborations between information behaviour scholars, cybersecurity experts, and human-computer interaction researchers can advance the design of digital environments that support adaptive information behaviours and resilience in the face of security threats.

### About the author(s)

**Hung Fai Joseph Cheng** is a research student at Swinburne University of Technology, Victoria, Australia. He holds a Bachelor of Social Science (Psychology), Bachelor of Engineering (Computer Science) and Graduate Certificate in Cyber Security and currently works as a cybersecurity professional. Joseph's research interests lie at the intersection of psychology and cybersecurity, focusing on human information behaviour in the digital era. Email: [josephcheng@swin.edu.au](mailto:josephcheng@swin.edu.au)

Associate Professor **Paul Scifleet** is an information systems scholar at Swinburne University of Technology whose research investigates information governance, information behaviour, and information practices in digital and AI-mediated environments. He focuses on how socio-technical systems shape the creation, use, and management of information, including risky or “dangerous” documents, with attention to accountability, safety, and information protection in complex digital ecosystems. Email: [pscifleet@swin.edu.au](mailto:pscifleet@swin.edu.au)

Dr **Misita Anwar** is an Information Systems researcher and educator at Swinburne University of Technology. Her work focuses on digital inclusion, socio-technical systems, and responsible technology in diverse communities. She has contributed to projects on cybersecurity awareness, participatory design, and community-centred innovation. Dr Anwar holds a PhD in the field of Information Technology from Monash University. Email: [misistaanwar@swin.edu.au](mailto:misistaanwar@swin.edu.au)

## References

- Agarwal, N.K. (2023). Information behavior research in the twenty-first century: The journey so far. *Information*. Vol. 28(1):97-146. <https://doi.org/10.35643/info.28.1.5>
- Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology*, 8(1), 19–32. <https://doi.org/10.1080/1364557032000119616>
- Auster, E., & Choo, C. W. (1993). Environmental scanning by CEOs in two Canadian industries. *Journal of the American Society for Information Science*, 44(4), 194–203. [https://doi.org/10.1002/\(SICI\)1097-4571\(199305\)44:4<194::AID-ASI2>3.0.CO;2-1](https://doi.org/10.1002/(SICI)1097-4571(199305)44:4<194::AID-ASI2>3.0.CO;2-1)
- Ayaburi, E. W. (2023). Understanding online information disclosure: Examination of data breach victimization experience effect. *Information Technology & People*, 36(1), 95–114. <https://doi.org/10.1108/ITP-04-2021-0262>
- Bada, M. & Nurse, J. (2019). The social and psychological impact of cyberattacks. In: V. Benson & J., McAlaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities*. London: Academic Press; (2019). p. 73–92. <https://doi.org/10.1016/B978-0-12-816203-3.00004-6>
- Barbour, J. B., Rintamaki, L. S., Ramsey, J. A., & Brashers, D. E. (2012). Avoiding health information. *Journal of Health Communication*, 17(2), 212–229. <https://doi.org/10.1080/10810730.2011.585691>
- Barnett, O. W., Martinez, T. E., & Keyson, M. (1996). The relationship between violence, social support, and self-blame in battered women, *Journal of Interpersonal Violence*, 11(2), 221–233. <https://doi.org/10.1177/088626096011002006>
- Belkin, N. J. (1990). The cognitive viewpoint in information science. *Journal of Information Science*, 16(1), 11–15. <https://doi.org/10.1177/016555159001600104>
- Brashers, D. E. (2001). Communication and uncertainty management. *Journal of Communication*, 51(3), 477–497. <https://doi.org/10.1111/j.1460-2466.2001.tb02892.x>
- Brashers, D. E., Goldsmith, D. J., & Hsieh, E. (2002). Information seeking and avoiding in health contexts. *Human Communication Research*, 28(2), 258–271. <https://doi.org/10.1111/j.1468-2958.2002.tb00807.x>
- Brashers, D. E., Neidig, J. L., Haas, S. M., Dobbs, L. K., Cardillo, L. W., & Russell, J. A. (2000). *Communication in the management of uncertainty: The case of persons living with HIV or AIDS*. *Communication Monographs*, 67(1), 63–84. <https://doi.org/10.1080/03637750009376495>
- Bryant, P. A. (2025). *The silent epidemic: Unseen factors driving data breach fatigue in everyday lives* [Doctoral dissertation, Temple University]. Temple University ScholarShare. <https://scholarshare.temple.edu/server/api/core/bitstreams/2d727ba5-8e59-42a8-971c-2a33beab6a24/content>
- Budimir, S., Pieh, C., Humer, E., & Probst, T. (2021). Comparing mental health during the COVID-19 lockdown and 6 months after the lockdown in Austria: A longitudinal study. *Frontiers in Psychiatry*, 12, Article 625973. <https://doi.org/10.3389/fpsyt.2021.625973>
- Bygrave, L. A. (2020). Data protection by design and by default: Deciphering the EU's legislative requirements. *Oslo Law Review*, 7(1), 105–120. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3035164](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3035164)

- Case, D. O., Andrews, J. E., Johnson, J. D., & Allard, S. L. (2005). Avoiding versus seeking: The relationship of information seeking to avoidance, blunting, coping, dissonance, and related concepts. *Journal of the Medical Library Association*, 93(3), 353.  
<https://pmc.ncbi.nlm.nih.gov/articles/PMC1175801/>
- Case, D. O., Given, L. M., & Willson, R. (2023). *Looking for information: Examining research on how people engage with information*. Emerald Publishing Limited.
- Cheng, C., Chan, L., Chau, C. L., (2020). Individual differences in susceptibility to cybercrime victimisation and its psychological aftermath. *Computers in Human Behavior*, 108.  
<https://doi.org/10.1016/j.chb.2020.106311>.
- Chu, H., & Liu, S. (2023). Risk-efficacy framework: Understanding the psychological mechanism of threat perception and behavioral intention. *Current Psychology*, 43, 5999–6012.  
<https://doi.org/10.1007/s12144-023-04813-9>.
- Cross, C., Richards, K., & Smith, R. (2016). *Improving responses to online fraud victims: An examination of reporting and support. Final report for Criminology Research Grant*, 29/13-14. Australian Institute of Criminology, Australia. <https://eprints.qut.edu.au/98346/>
- Cross, C., & Holt, T. J. (2025). *Beyond fraud and identity theft: Assessing the impact of data breaches on individual victims*. *Journal of Crime and Justice*. Advance online publication.  
<https://doi.org/10.1080/0735648X.2025.2535007>
- Czeisler, M. É., Marynak, K., Clarke, K. E. N., Salah, Z., Shakya, I., Thierry, J. M., Ali, N., McMillan, H., Wiley, J. F., Weaver, M. D., Czeisler, C. A., Rajaratnam, S. M. W., & Howard, M. E. (2020). Delay or avoidance of medical care because of COVID-19-related concerns – United States, June 2020. *MMWR. Morbidity and Mortality Weekly Report*, 69(36), 1250–1257. DOI: <http://dx.doi.org/10.15585/mmwr.mm6936a4>
- Data Protection Act 2018, c. 12. <https://www.legislation.gov.uk/ukpga/2018/12/contents>
- Davies, K., & Harrison, J. (2007). The information-seeking behaviour of doctors: A review of the evidence. *Health Information and Libraries Journal*, 24(2), 78–94.  
<https://doi.org/10.1111/j.1471-1842.2007.00713.x>
- Delker, B. C. (2022). *Interpersonal violence in context: A call to consider cultural stigma in theory and research on the psychology of trauma*. In K. C. McLean (Ed.), *Cultural methods in psychology: Describing and transforming cultures* (pp. 356–386). Oxford University Press.  
<https://doi.org/10.1093/oso/9780190095949.003.0012>
- Delker, B. C., Salton, R., & McLean, K. C. (2019). Giving voice to silence: Empowerment and disempowerment in the developmental shift from trauma ‘victim’ to ‘survivor-advocate.’ *Journal of Trauma & Dissociation*, 21(2), 242–263.  
<https://doi.org/10.1080/15299732.2019.1678212>
- Dervin, B. & Nilan, M. (1986). Information needs and uses. *Annual Review of Information Science and Technology*, 21, 3–33.
- Earnshaw, V. A., & Chaudoir, S. R. (2009). From conceptualizing to measuring HIV stigma: A systematic review. *AIDS and Behavior*, 13(6), 1160–1177. <https://doi.org/10.1007/s10461-009-9593-3>
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

- (General Data Protection Regulation). *Official Journal of the European Union*. L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford University Press.
- Fisher, K. E., Erdelez, S., & McKechnie, L. (Eds.). (2005). *Theories of information behavior*. Information Today, Inc.
- Fischer, P., Jonas, E., Frey, D., & Schulz-Hardt, S. (2005). Selective exposure to information: The impact of information limits. *European Journal of Social Psychology*, 35(4), 469–492. <https://doi.org/10.1002/ejsp.264>
- Foust, J. L., & Taber, J. M. (2023). Information avoidance: Past perspectives and future directions. *Perspectives on Psychological Science*, 20(2), 241–263. <https://doi.org/10.1177/17456916231197668>
- Foust, J. L., & Taber, J. M. (2024). Injunctive social norms and perceived message tailoring are associated with health information seeking. *Journal of Behavioral Medicine*, 47(1), 1–14. <https://doi.org/10.1007/s10865-023-00413-x>
- Golladay, K., & Holtfreter, K. (2016). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, 12(5), 741–760. <https://doi.org/10.1080/15564886.2016.1177766>
- Golman, R., Hagmann, D., & Loewenstein, G. (2017). Information avoidance. *Journal of Economic Literature*, 55(1), 96–135. <https://doi.org/10.1257/jel.20151245>
- Hart, W., Albarracín, D., Eagly, A. H., Brechan, I., Lindberg, M. J., & Merrill, L. (2009). Feeling validated versus being correct: A meta-analysis of selective exposure to information. *Psychological Bulletin*, 135(4), 555–588. <https://doi.org/10.1037/a0015701>
- Hay, C. and Ray K. (2019). General Strain Theory and Cybercrime. In *The Palgrave handbook of international cybercrime* (pp. 584–597). Palgrave Macmillan, Cham.
- Hayes, S. C., Wilson, K. G., Gifford, E. V., Follette, V. M., & Strosahl, K. (1996). Experiential avoidance and behavioral disorders: A functional dimensional approach to diagnosis and treatment. *Journal of Consulting and Clinical Psychology*, 64(6), 1152–1168. <https://doi.org/10.1037/0022-006X.64.6.1152>
- Herman, J. (2015). *Trauma and recovery: The aftermath of violence—from domestic abuse to political terror*. Basic Books/Hachette Book Group.
- Hicks, A., McKenzie, P., Bronstein, J., Hyldegård, J. S., Ruthven, I., & Widén, G. (2024). Information avoidance: A critical conceptual review. *Journal of the Association for Information Science and Technology*, 76(1), 326–346. <https://doi.org/10.1002/asi.24968>
- Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), Article 7. <https://doi.org/10.5817/CP2016-4-7>
- Howell, J. L., Ratliff, K. A., & Shepperd, J. A. (2016). Automatic attitudes and health information avoidance. *Health Psychology*, 35(8), 761–766. <https://doi.org/10.1037/hea0000330>
- Howell, J. L., & Shepperd, J. A. (2012). Reducing information avoidance through affirmation. *Psychological Science*, 23(2), 141–145. <https://doi.org/10.1177/0956797611424164>

- Howell, J. L. & Shepperd, J. A. (2013). Behavioral obligation and information avoidance. *Annals of Behavioral Medicine*, 45(2), 258-263. <https://doi.org/10.1007/s12160-012-9451-9>
- Hurtado, S., Marine, S. & McCoy-Simmons, C. (2021). Survivor-faculty: Making meaning of identity and putting identity into action. *The Journal of the Professoriate*, (12)2, 57-81. <https://morgridge.du.edu/sites/default/files/2023-06/Survivor-Faculty.pdf>
- Huvila, I., & Gorichanaz, T. (2025). Trends in information behavior research, 2016–2022: An Annual Review of Information Science and Technology (ARIST) paper. *Journal of the Association for Information Science and Technology*, 76(1), 216–237. <https://doi.org/10.1002/asi.24943>
- Hytönen, E., Trent, A., & Ruoslahti, H. (2022). Societal impacts of cyber security in academic literature – Systematic literature review. In *Proceedings of the 21st European Conference on Cyber Warfare and Security* (pp. 86–93). <https://doi.org/10.34190/eccws.21.1.288>
- Internet Crime Complaint Center (IC3). (2024). *Internet crime report 2024*. [https://www.ic3.gov/AnnualReport/Reports/2024\\_IC3Report.pdf](https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf)
- Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Qualitative Criminology*, (6)2, 5. <https://dc.swosu.edu/qc/vol6/iss2/5>
- Kaakinen, M. (2018). Shared identity and shared information in social media: Development and validation of the identity bubble reinforcement scale. *Media Psychology*, 21(3), 394-420. <https://doi.org/10.1080/15213269.2018.1544910>
- Kaminska, M., & Duquette, A. (2021). Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. *Journal of Cybersecurity*, 7(1). <https://doi.org/10.1093/cybsec/tyab007>
- Kamkar, K. & Duquette, R. (2021, April 16). Psychological trauma and cybercrime. *Canadian Occupational Safety*, <https://www.thesafetymag.com/ca/news/opinion/psychological-trauma-and-cybercrime/252447>
- Karlsson, N., Loewenstein, G., & Seppi, D. (2009). The ostrich effect: Selective attention to information. *Journal of Risk and Uncertainty*, 38, 95–115. <https://doi.org/10.1007/s11166-009-9060-6>
- Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the Capital One data breach: Critical lessons learned. *ACM Transactions on Privacy and Security*, 26(1), 1–29. <https://doi.org/10.1145/3546068>
- Kilovaty, I. (2021). Psychological Data Breach Harms. *North Carolina Journal of Law & Technology*, 23(1). [http://journals.law.unc.edu/ncjolt/wp-content/uploads/sites/4/2021/10/NCJOLT-Vol.23.1\\_1-66\\_Kilovaty.pdf](http://journals.law.unc.edu/ncjolt/wp-content/uploads/sites/4/2021/10/NCJOLT-Vol.23.1_1-66_Kilovaty.pdf)
- Kirlappos, I., Beaument, A., Sasse, M.A. (2013). “Comply or die” is dead: Long live security-aware principal agents. In: Adams, A.A., Brenner, M., Smith, M. (Eds.), *Financial Cryptography and Data Security*. FC 2013. Lecture Notes in Computer Science, vol 7862. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-642-41320-9\\_5](https://doi.org/10.1007/978-3-642-41320-9_5)
- Koch, H. and Adeleye, N. (2019). Psychological injury, cyber crime and data breach damages. *The Expert Witness Journal*, 26, 53-55. <https://www.open-access.bcu.ac.uk/id/eprint/5899>

- LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3), 71–76. <https://doi.org/10.1145/1325555.1325569>
- Legal Information Institute. (2025). *Consumer protection laws*. Cornell Law School. [https://www.law.cornell.edu/wex/consumer\\_protection\\_laws](https://www.law.cornell.edu/wex/consumer_protection_laws)
- Lévai, T., Lázár, G., Krajnovic, E. (2024). Examining illness narratives in the context of the postoperative psychological state: A mixed-methods study of emotion-focused illness narrative. *BioPsychoSocial Medicine*, 18,21. <https://doi.org/10.1186/s13030-024-00318-4>
- Li Y., Yazdanmehr A., Wang J., Rao H. R. (2019). Responding to identity theft: A victimization perspective. *Decision Support Systems*, 121, 13–24. <https://doi.org/10.1016/j.dss.2019.04.002>
- Liu, F. (2022). *Irrational human factors in behavioral information security: Familiarity, fear, and a change of mind*. [Doctoral Dissertation, University of Jyväskylä]. JYU. <https://urn.fi/URN:ISBN:978-951-39-9090-9>
- Liu, K., & Chen, M. (2024). Disentangling the effects of cognitive, affective, and sociocultural factors on risk information avoidance: A meta-analysis. *Communication Research*, 53(3). <https://doi.org/10.1177/00936502241246513>
- Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, 34, 754–772. <https://doi.org/10.1016/j.clsr.2018.05.017>.
- Mateu, A., Pascual-Sánchez, A., Martinez-Herves, M. (2020). Cyberbullying and post-traumatic stress symptoms in UK adolescents. *Archives of Disease in Childhood*, 105(10), 951–956. <https://doi.org/10.1136/archdischild-2019-318716>
- Mayer, P., Zou, Y., Lowens, B. M., Dyer, H. A., Le, K., Schaub, F., & Aviv, A. J. (2023). Awareness, intention, (In)Action: Individuals' Reactions to Data Breaches. *ACM Transactions on Computer-Human Interaction*, 30(5), 1–53. <https://doi.org/10.1145/3589958>
- Mayer, P., Zou, Y., Schaub, F., & Aviv, A. J. (2021). "Now I'm a bit angry." Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *30th USENIX Security Symposium (USENIX Security 21)*, 393–410. <https://www.usenix.org/system/files/sec21-mayer.pdf>
- Melnyk, D., & Shepperd, J. A. (2012). Avoiding risk information about breast cancer. *Annals of Behavioral Medicine*, 44(2), 216–224. <https://doi.org/10.1007/s12160-012-9382-5>
- Miller, S. M., & Mangan, C. E. (1983). Interacting effects of information and coping style in adapting to gynaecological stress: Should the doctor tell all? *Journal of Personality and Social Psychology*, 45, 223–236. <https://doi.org/10.1037//0022-3514.45.1.223>
- Muzatko, S. & Bansal, G. (2024). It pays to be forthcoming: timing of data breach announcement, trust violation, and trust restoration. *Internet Research*, 34(5), 1629–1663. <https://doi.org/10.1108/INTR-12-2021-0939>
- Narayan, B., Case, D. O., & Edwards, S. L. (2011). The role of information avoidance in everyday-life information behaviors. *Proceedings of the American Society for Information Science and Technology*, 48(1), 1–9. <https://doi.org/10.1002/meet.2011.14504801085>
- Nurse, J. R. C. (2018). *Cybercrime and you: How criminals attack and the human factors that they seek to exploit*. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Eds.), *The Oxford*

- handbook of cyberpsychology. Oxford University Press.  
<https://doi.org/10.1093/oxfordhb/9780198812746.013.35>
- Neal, T. M. S., MacLean, N., Morgan, R. D., & Murrie, D. C. (2024). Confirmatory information seeking is robust in psychologists' diagnostic reasoning. *Law and Human Behavior*, 48(5-6), 503-518. <https://doi.org/10.1037/lhb0000574>
- Nickerson, R.S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2, 175-220. <https://doi.org/10.1037/1089-2680.2.2.175>
- Nobles, C. (2022). Stress, burnout and security fatigue in cybersecurity: A human factors problem, *HOLISTICA - Journal of Business and Public Administration*, 13(1), 49-72.  
<https://doi.org/10.2478/hjbpa-2022-0003>
- Office of the Australian Information Commissioner. (2025a). OAIC regulatory priorities 2025-26. <https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/oaic-regulatory-priorities>
- Office of the Australian Information Commissioner. (2025b). Notifiable data breaches report: July to December 2024. <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2024>
- Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An exploration of the psychological impact of hacking victimization. *SAGE Open*, 11(4). <https://doi.org/10.1177/21582440211061556>
- Park, S., Fisher, C., Fletcher, R., Tandoc Jr, E., Dulleck, U., Fulton, J., Stepnik, A., & Yao, S. P. (2024). Exploring responses to mainstream news among heavy and non-news users: From high-effort pragmatic scepticism to low-effort cynical disengagement. *New Media & Society*, 27(7). <https://doi.org/10.1177/14614448241234916>
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), 597-611. <https://doi.org/10.1016/j.cose.2011.12.010>
- Qi, J., Han, Z., & Hansen, P. (2024). Information search process model based on costs and benefits: A behavioural economics perspective. *Journal of Documentation*, 80(6), 1494-1507.  
<https://doi.org/10.1108/JD-12-2023-0259>
- Rhoads, J. (2023). Psychological effects of cybercrime on minorities: Short-term and long-term impacts. *Journal of Empirical Social Science Studies*, 7(1), 1-31.  
<https://publications.dlpress.org/index.php/jesss/article/view/3>
- Riek, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13(2), 261-273. <https://doi.org/10.1109/TDSC.2015.2410795>
- Sairanen, A. and Savolainen, R. (2010). Avoiding health information in the context of uncertainty management. *Information Research*, 15,4. <https://core.ac.uk/reader/250142040>
- Sargiotis, D. (2024). Legal and regulatory considerations in data governance. In: *Data Governance*. Springer, Cham. [https://doi.org/10.1007/978-3-031-67268-2\\_15](https://doi.org/10.1007/978-3-031-67268-2_15)
- Savolainen, R. (2017). Information need as trigger and driver of information seeking: A conceptual analysis. *Aslib Journal of Information Management*, 69(1), 2-21.  
<https://doi.org/10.1108/AJIM-08-2016-0139>
- Schiliro, F. (2023). Towards a Contemporary Definition of Cybersecurity. 10.48550/arXiv.2302.02274.

- Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic data privacy law. *Georgetown Law Journal*, 106(1), 115–179. <https://www.law.georgetown.edu/georgetown-law-journal/in-print/volume-106/volume-106-issue-1-november-2017/transatlantic-data-privacy-law/>
- Sears, C. R., & Cunningham, D. R. (2024). Individual differences in psychological stress associated with data breach experiences. *Journal of Cybersecurity and Privacy*, 4(3), 28. <https://doi.org/10.3390/jcp4030028>
- Shandler, R., Gross, M. L., & Canetti, D. (2023). Cyberattacks, psychological distress, and military escalation: An internal meta-analysis. *Journal of Global Security Studies*, 8(1), 1–19. <https://doi.org/10.1093/jogss/ogac042>
- Smith, S. M., Fabrigar, L. R., & Norris, M. E. (2008). Reflecting on six decades of selective exposure research: Progress, challenges, and opportunities. *Social and Personality Psychology Compass*, 2(1), 464–493. <https://doi.org/10.1111/j.1751-9004.2007.00060.x>
- Solove, D. J., & Citron, D. K. (2016). Risk and anxiety: A theory of data breach harms. *SSRN Electronic Journal*. 96(4). DOI:[10.2139/ssrn.2885638](https://doi.org/10.2139/ssrn.2885638)
- Solove, D. J., & Citron, D. K. (2017). *Privacy and the new media: Law and practice*. Aspen Publishers.
- Spink, A., & Cole, C. (2004). A human information behaviour approach to a philosophy of information. *Library Trends*, 52(3), 617–628. <http://hdl.handle.net/2142/1690>
- Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT professional*, 18(5). <https://doi.org/10.1109/mitp.2016.84>
- Sultana, T., Dhillon, G., & Oliveira, T. (2023). The effect of fear and situational motivation on online information avoidance: The case of COVID-19. *International Journal of Information Management*, 66, 102489. <https://doi.org/10.1016/j.ijinfomgt.2022.102596>
- Sutton, S. A. (1994). The role of attorney mental models of law in case relevance determinations: An exploratory analysis. *Journal of the American Society for Information Science*, 45(3), 186–200. [https://doi.org/10.1002/\(SICI\)1097-4571\(199404\)45:3<186::AID-ASI8>3.0.CO;2-F](https://doi.org/10.1002/(SICI)1097-4571(199404)45:3<186::AID-ASI8>3.0.CO;2-F)
- Sweeny, K., Melnyk, D., Miller, W., & Shepperd, J. A. (2010). Information avoidance: Who, what, when, and why. *Review of General Psychology*, 14(4), 340–353. <https://doi.org/10.1037/a0021288>
- Taber, J.M., Leyva, B. & Persoskie, A. (2015). Why do people avoid medical care? A qualitative study using national data. *Journal of General Internal Medicine*, 30, 290–297. <https://doi.org/10.1007/s11606-014-3089-1>
- Tsang, S.J. (2017). Cognitive discrepancy, dissonance, and selective exposure. *Media Psychology*, 22(3), 394–417. <https://doi.org/10.1080/15213269.2017.1282873>
- van Dijk, J. A. G. M. (2020). *The digital divide*. Cambridge, UK; Medford, MA: Polity Press.
- Velmans, M. (1991). Is human information processing conscious? *Behavioral and Brain Sciences* 14(4). <https://doi.org/10.1017/S0140525X00071776>
- Verizon (2023). 2023 Data breach investigations report. Verizon. <https://verizon.com/dbir>.
- Voce, I., & Morgan, A. (2023). Online behaviour, life stressors and profit-motivated cybercrime victimisation. *Trends & Issues in Crime and Criminal Justice*, No. 675. Canberra: Australian Institute of Criminology. <https://doi.org/10.52922/ti77062>

- Wang, Y., Ahmed, S., & Bee, A. W. T. (2024). Selective avoidance as a cognitive response: Examining the political use of social media and surveillance anxiety in avoidance behaviours. *Behaviour & Information Technology*, 43(3), 590–604. <https://doi.org/10.1080/0144929X.2023.2182609>
- Whitson, T. & Davis, L. (2001). Best practices in electronic government: Comprehensive electronic information dissemination for science and technology, *Government Information Quarterly*, 18(2), 79–91. [https://doi.org/10.1016/S0740-624X\(01\)00062-4](https://doi.org/10.1016/S0740-624X(01)00062-4)
- Zaeifi, M., Kalantari, F., Oest, A., Sun, Z., Ahn, G., Shoshitaishvili, Y., Bao, T., Wang, R., & Doupé, A. (2024). Nothing personal: Understanding the spread and use of personally identifiable information in the financial ecosystem. *CODASPY '24: Fourteenth ACM Conference on Data and Application Security and Privacy*. <https://doi.org/10.1145/3626232.3653266>
- Zhu, Q., Weeks, B. E., & Kwak, N. (2024). Implications of online incidental and selective exposure for political emotions: Affective polarization during elections. *New Media & Society*, 26(1), 450–472. <https://doi.org/10.1177/14614448211061336>
- Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018). "I've got nothing to lose": Consumers' risk perceptions and protective actions after the Equifax data breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 197–216. <https://www.usenix.org/system/files/conference/soups2018/soups2018-zou.pdf>

© [CC-BY-NC 4.0](#) The Author(s). For more information, see our [Open Access Policy](#).