Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

No. 731 July 2026

Abstract | This study uses data from online moderated interviews with 33 ransomware victims to examine victim decision-making during a ransomware attack.

While ransomware attacks could be a fear-inducing and stressful experience, victims logically assessed the threat and weighed up their responses. Victims commonly found practical ways to restore their data and systems, often with advice and support from trusted sources.

Victims rarely tried to negotiate with offenders. The vast majority of victims decided against paying the ransom because they distrusted the offenders.

Victims are capable of rational decision-making following ransomware attacks even during periods of heightened stress and emotion. Support and resources to help victims assess the risks associated with a ransomware attack and to restore their data and devices must be readily accessible when ransomware attacks occur.

Victim decision-making during ransomware attacks

Isabella Voce and Anthony Morgan

Ransomware is a highly destructive and pervasive threat that involves the use of malware to encrypt data or systems and extort victims (Australian Signals Directorate 2024). Ransomware attacks involve criminal actors infiltrating a victim's computer, network or device, then locking or encrypting their data or making their system non-functional, before demanding the victim pay a ransom for their data or systems to be restored (Institute for Security and Technology 2021).

Ransomware research has generally focused on the technical aspects of these attacks, such as the techniques used by offenders or the features of the malware; however, there is an important human element (Matthijsse, Van 't Hoff-de Goede & Leukfeldt 2023). The success of a ransomware attack, and the ransomware business model, relies on both the strength of the encryption and the cybercriminal's ability to persuade the victim to pay the ransom (McIntyre & Frank 2021). Some recent research has focused on the latter, with crime script analysis by Matthijsse, Van 't Hoff-de Goede and Leukfeldt (2023) and interviews with victims and police by Connolly and Borrion (2022) examining human involvement and decision-making in ransomware attacks, highlighting how victim decisions and actions influence the ransomware process.

Ransomware attacks often originate from phishing, insecure or spoofed websites, social media and malicious advertisements (Matthijsse, Van 't Hoff-de Goede & Leukfeldt 2023; Voce & Morgan 2025). Once the system or device has been infected and data encrypted or stolen (a growing practice), a ransom message will be displayed (Matthijsse, Van 't Hoff-de Goede & Leukfeldt 2023). Victims will notice signs such as their desktop being locked, files going missing and common applications crashing or not opening (Hull, John & Arief 2019). In rare cases, offenders will carry out multi-extortion ransomware schemes where they also pressure the victims with distributed denial-of-service attacks or by communicating directly with the victim's customers and stakeholders (Meurs 2025).

Victims must then decide whether to pay the ransom. The current advice from the Australian Government is that victims should never pay to resolve ransomware attacks. Paying does not guarantee that their data will be restored or will not be sold or leaked online, and it can increase their chances of being targeted by another attack (Australian Signals Directorate nd). But many factors can influence this decision for victims, including whether the demands being made by the cybercriminals seem genuine, whether data could be retrieved, the advice received by victims, whether the victim can afford the ransom and whether it will result in further attacks (Connolly & Borrion 2022; Voce & Morgan 2021). Offenders can exert pressure on victims to pay, give instructions on how to buy cryptocurrency, negotiate the payment deadline or amount, and attempt to demonstrate they can and will decrypt the data upon payment (Connolly & Borrion 2022; Matthijsse, Van 't Hoff-de Goede & Leukfeldt 2023).

Different decision-making models can help us understand the victim response to ransomware attacks. Dual processing theory suggests there are two modes of decision-making (Kahneman 2003). System 1 thinking is fast, automatic, led by emotion, and beneficial for quickly arriving at a choice with limited information. System 2 is slower, analytical, requires conscious effort and situational information, and is better at evaluating alternative options to identify the ideal choice (Kahneman 2011). Criminal actors use aggressive tactics during ransomware attacks to induce System 1 processing and increase the likelihood of victim compliance. Actors will limit the time for victims to make decisions, with attention-grabbing cues such as countdown timers (Patyal et al. 2017), which can induce stress and fear, coercing victims to make decisions quickly without exploring all options. High levels of negative emotion can load a victim's cognitive capacity and interfere with their decision-making ability (Angie et al. 2011; Bartholomeyczik, Gusenbauer & Treffers 2022).

Rational choice models, which have primarily focused on offender decision-making, suggest that individuals use objective calculations (ie System 2 thinking) to make rational decisions in line with their personal objectives and self-interest (Cornish & Clarke 2014). Victims are also rational actors, who make decisions using the information available to them (Meyer 2012). This decision-making may involve cost–benefit analysis, or weighing up the actual or perceived benefits, costs and risks. Prior research indicates that ransomware victims often perform a cost–benefit analysis before deciding whether to pay the requested ransom (Connolly & Borrion 2022). However, this research focused on organisations rather than individual victims, and involved a small number of victim interviews. More research is needed to understand the decision-making of individual victims from their own perspective, including the interaction between System 1 and System 2 thinking and the role that threats, coercion, stress and emotion play in shaping decision-making. This can inform efforts to assist victims during an attack and reduce the viability of the ransomware business model.

Method

This study uses data from online moderated interviews to examine victim decision-making during a ransomware attack and what factors influence these decisions. We examine ransomware attacks from the perspective of victims, to understand how they assess the threat and decide what action to take in response. The sample for this study was drawn from a larger survey of online Australians about their experiences of cybercrime (Voce & Morgan 2023). Respondents were asked whether:

- their devices, servers, service or networks had been disrupted and they received instructions for paying a ransom to restore functionality;
- their systems, devices or files had a virus or became inaccessible and they received instructions for paying a ransom to restore access; or
- they received a ransom message on their device to say their data or information had been stolen and they had to pay to prevent this information from being leaked or sold online.

Respondents who reported that they had experienced any of these incidents in the past year were then asked whether they would be willing to participate in follow-up online questioning, in which a moderator posed questions and prompts to respondents, to better understand their experiences of ransomware victimisation. After recruitment, interviews were undertaken with 33 participants about the most recent ransomware attack they had experienced, including their perceptions of what happened before, during and after the attack. Because some respondents had experienced multiple ransomware incidents in the past year, the moderated interview focused on the most recent incident. Most of the sample were male (*n*=21, 64%) and had experienced a ransomware incident that was not work related (*n*=20, 61%) meaning the attack did not involve work-related devices, systems and email accounts. Thirty percent of respondents were aged 25 to 39 years old (*n*=10), 24 percent were aged 40 to 54 years old (*n*=8), 33 percent were aged 55 to 69 years old (*n*=11) and 12 percent were aged 70 years or over (*n*=4).

Interviews were undertaken using an interactive, text-based online platform managed by market research company Roy Morgan. The semi-structured questionnaire included a series of open-ended questions that allowed participants to describe their experience, with some additional prompting from the moderator. Participants were asked to describe their actions and thoughts throughout the process of receiving the message, during and after the attack. Our analysis focused on how they appraised the ransomware threat, the actions they took to respond to the threat, and the reasons behind their decision about whether or not to pay the ransom. We adopted an inductive approach to identify the most common themes to emerge from the online interviews. As this was a written interview, we have presented the written responses verbatim, retaining grammatical and spelling errors.

Limitations

While most participants were forthcoming, requiring relatively little prompting, some may have been reluctant to share information about their ransomware victimisation, particularly if the incident involved their workplace or if they felt responsible for the attack. Using a confidential online platform ensured the identity of participants was unknown to the moderators, which may have helped to increase participation. However, having the interview in a written format limited our ability to explore issues in depth, and may have caused participants to give less detailed answers then they would have given in a spoken interview. In particular, only one respondent openly talked about making the ransomware payment, which limited our ability to examine why victims decided to pay (as opposed to the reasons for not paying). As with any qualitative study, we are cautious about generalising beyond the sample of individuals who participated in the research.

Results

Victim appraisal of the threat

Victims typically received the ransom messages over email, while a small number received text messages or pop-up messages on their computer screen or found text files in the folders of their device. The ransom messages claimed that the attackers accessed the victim's devices, systems and/or data, and the victim had to pay to restore device or system functionality, and/or prevent data being shared or sold online. Whether victims assessed these threats to be genuine and serious depended predominantly on evidence of system, device and file impacts. Many victims quickly identified impacts, including that their files had been altered or encrypted, their personal information had been accessed, malware had been installed on the device, or the device was being remotely controlled by the attackers.

> In the morning I found the PC had not shutdown, was still usable but virtually all, but essential programs, would not run and no data could be accessed. Examining the system I found that virtually all data files in the PC and attached drives appeared to have been encrypted and their file type changed to access. Additionally I found an identical text message in every folder advising of the encryption and providing an email address should I wish to have all the data unencrypted. (Respondent 12)

> … my computer had been affected badly. The data had been altered as well as leak of personal information such as name, bank account. There was also virus on my computer which made the computer mouse moving uncontrollably. (Respondent 2)

Victims were also asked how they believed their devices became infected with malware. Some victims had clicked on a suspicious link or attachment in an email or on a website, which they believed to be the cause of the malware.

> I actually clicked to the link appeared on the screen when I access the website. (Respondent 2)

> I was going through my emails and stupidly clinked on a dodgy link (looked link Amazon), this locked me out of most of my computer (Respondent 23)

The ransom messages contained demands typical of ransomware attacks. According to victims, the ransom messages usually demanded several hundred dollars and gave them between 48 hours and seven days to make the payment. Some messages warned victims not go to authorities or seek other assistance, thereby attempting to isolate the victim and keep them uninformed.

> $510 US equivalent in Bitcoin within two days. I was told not to notify authorities about any of this, and that unless I paid I would also lose all the data on my computer. (Respondent 21)
>
> … demanded payment in Bitcoin (I forget the quantity) be made within 7 days and provided a wallet-id. It did warn me not to contact authorities. (Respondent 8)

Including the victim's personal information was another tactic attackers used to convince victims that their systems and information had been compromised, and to increase the perceived severity of the threat. Attackers cited victims' names, email addresses and the current or former passwords for various accounts. A few respondents believed this personal information had been leaked through third-party data breaches.

> I assumed that the email was sent to me as a result of the hacking of the website and data breach of my health insurance company … The sender of the email, by effort to demonstrate proof, provided a 'near' reproduction of my password(s). Close, but not quite. (Respondent 11)

Some victims who believed their information had been leaked from a third party realised their personal devices and systems had likely not been accessed, and the ransom messages were probably opportunistic empty threats. This assessment was made in conjunction with other factors, such as whether the personal information was outdated and whether they saw evidence of device or system impacts. Usually, these victims deleted the ransom messages and took precautionary security measures such as changing passwords and running virus scans.

> It was the original password when I had set up the email account with my internet provider in 2003 and I had never changed it … I changed the password on my email account and deleted the messages … Nothing on my computer was effected. (Respondent 5)
>
> The perpetrator somehow had some of my old data, including old passwords but they did not have much more than that. (Respondent 31)

The advice given to victims at this early assessment phase was important to victims in deciding the legitimacy of the threat.

> I spoke to my IT Department as well as a friend. I was put at ease by this and decided that I was being scammed to pay up and that they only had old and no longer used data. (Respondent 31)

Participants described strong emotional responses to seeing impacts on their devices and systems, including panic, anger and sometimes self-blame.

> My immediate response was disbelief, I couldn't believe that I had been stupid enough to click on something that let them in. Then I was angry and felt violated knowing they had stolen files and altered files so I couldn't access my data. (Respondent 9)
>
> My immediate response was a rush of panic. Seeing my screen taken over by that ominous message, with the demand for payment and the threats, felt like a surreal nightmare. I think a part of me wanted to believe it was some kind of hoax or prank, but the realization that my files were inaccessible confirmed the severity of the situation. (Respondent 16)

The ransom messages sometimes included several features designed to make the victim take the threats seriously and experience urgency and fear. The messages often limited the time in which to make a payment and had an ominous tone, with threatening language, a black screen, red font and skull images.

> It was such a nightmare. ☹ I remember the message vividly—it popped up on my screen in a big red font, like something out of a hacker movie … The message came through as a creepy pop-up window, accompanied by a scary-looking skull icon. (Respondent 16)
>
> I was casually browsing internet news when the screen of my laptop just froze. The big sign in red appeared on the screen with a landline number to call immediately … The experience was so scary and frightening (Respondent 32)

Another tactic that caused victims fear and stress was including their personal data in the ransom messages, as victims could not be sure what information was available online or had been obtained by the criminals.

> The perpetrator spelled out a password of mine in the email text so it was obvious that my personal information had been compromised. I used apple and google to check my details and found that my email was involved in many data breaches, which was disappointing to see … Immediately I panicked. I thought "gee what are they going to do". For a split second I even considered if I should pay the money. (Respondent 13)
>
> I was very alarmed and frightened. It's the first time I felt fully exposed online and thought deeply about how much risk I could be exposed to. (Respondent 6)

Victim responses to the threat

Victims who assessed the threat as genuine then took action to resolve or mitigate the situation. Some victims were able to restore the stolen or encrypted data and remove the malware from their systems. Most were unable to restore all of their files but could minimise the damage to an acceptable extent. This meant they did not need to pay the ransom, and the only cost was the time and effort they put into resolving the situation. These victims often had proactive cybersecurity practices—particularly regular automatic backups—and implemented post-incident security measures such as resetting passwords and using antivirus software. A few of these victims had expertise in IT security, followed workplace guidelines for handling cybercrime incidents or found information online.

> All systems were cleaned and restored without significant issue other than lost time (Respondent 10)
>
> The data was fully recovered, largely through the use of a pre-prepared written procedure for recovery, courtesy of the company that I work for, and a quick walk-through of the recovery process by a colleague who had similar issues … I believed that I would be able to fully recover all important information without having to consider paying a ransom. (Respondent 8)

Despite the attackers warning victims against seeking help with the ransomware attack, most victims did seek advice and support from a person or organisation they knew. This was usually friends, work colleagues or family who worked in the IT industry or were known by the victim to be tech-savvy. They provided practical advice on IT solutions and encouraged the victims to make formal reports to government agencies, police agencies and workplace IT departments.

> I contacted a close friend who works in IT security and explained the situation to them. They strongly advised me to report the incident to both the local law enforcement agency and my workplace's IT department … My workplace's IT department took immediate action to isolate the affected device and assess the extent of the breach. They also provided guidance on steps to take to minimize further damage and vulnerabilities. (Respondent 16)

> I contacted my two adult sons, both of whom work in the computer industry. They knew exactly what had happened, told me not to respond to the emails, and came and reimaged my computer, put a new password on the router, and recovered most of my files from a backup. (Respondent 9)

Few victims reported to formal sources such as the police and Scamwatch. For one victim, reporting to police was crucial for creating a record of the incident, should a formal investigation begin. The severity of the attack meant they chose to seek formal law enforcement advice despite the attackers' warnings.

> During the attack, seeking support and assistance was a complex decision. I was torn between the urgency of the situation and the warnings in the ransom message against involving authorities or anyone else. However, the severity of the attack ultimately led me to reach out for help … While the attackers warned against involving authorities, it was crucial to have a paper trail and official record of the attack … in terms of ensuring the attack was documented and that there was a trail of evidence for any potential investigation. (Respondent 16)

Several victims did not seek assistance or advice from anyone because they felt responsible, did not know who could help, believed the incident was not serious enough, or believed the offenders could not be caught.

> No I didn't contact anyone or asked for any help. I don't really feel that the police etc would really take any action. I feel that this is something that could be very difficult because the internet is so broad and is hard to regulate like if it were to be from something overseas. I think unless it's something extremely bad/severe or to happen to many people then they would take the appropriate action. (Respondent 15)

> I did not go to anyone else as at the time, I felt this was my fault for being silly enough to click on a link like that. (Respondent 23)

> I didn't go to anyone for support as I was not sure who would be able to support me. (Respondent 14)

Few victims communicated with the attackers in an attempt to understand the situation and negotiate a reduced payment, as most victims simply did not trust them.

> No interaction at all with the thieving, scamming arseholes. I don't respond well to threats … I did not negotiate with the scum. I don't negotiate with blackmailers. (Respondent 4)
>
> I chose not to reply or attempt any kind of negotiation. I didn't want to give them any more information or leverage than they already had. (Respondent 16)

For one victim who contacted the attackers, the attackers offered to decrypt one file as proof that they could and would decrypt the files upon payment, and also offered to reduce the payment amount. However, the victim was unconvinced the cybercriminals could be trusted, and still deemed the new amount to be too high given the risk that the data would not be recovered.

> I contacted the attacker and we exchanged several emails where we discussed a possible payment and a possible reduction of the initial demand made. A minor price reduction was achieved but at no stage was I ever convinced that any real possibility of having our data unencrypted and simply gave up contact … I was also advised that I could have one 'non essential' file unencrypted as proof that my files could all be unencrypted should I agree pay an amount in bitcoin (Respondent 12)

In another case, the victim called the attackers, who negotiated with the victim by offering to reduce the payment amount. The victim was able to convince the attackers that he genuinely could not afford any payment, and the criminal restored the computer and ended the attack.

> I Explained to him that the amount he is talking about is totally impossible. He said ok., I like you, just pay $500 and I'll fix your 'Life'. I'm quite sure he was seeing me on my laptop's camera. Only when I explained in detail my financial situation (unemployed, old and broke) and the fact that I'm renting he suddenly said ok, Next time you won't be so lucky. My computer was back to normal in a minute … I suspect he managed to see my ANZ bank account with $15 in it. And that was my salvation. (Respondent 32)

Victim decisions on ransom payment

All victims, except one, decided against making the ransom payment. Victims identified possible negative effects of paying and ultimately decided the downsides outweighed the potential benefits. Victims often acknowledged that paying the ransom would not guarantee that their systems would be restored, expressing distrust that the criminals would uphold their end of the deal.

> I had read enough about ransomware attacks to know that paying the ransom doesn't guarantee the safe return of your data. There are countless cases where victims paid up but didn't get their files decrypted or had their data exposed anyway. So, there was a significant level of distrust in whether the attackers would actually hold up their end of the bargain. (Respondent 16)
>
> I did not pay the random [sic] mainly because I don't trust that even if I paid the random [sic] that they would allow me to get my files back. (Respondent 14)

Some also knew that paying could actually increase their chances of being targeted again, either by demonstrating their willingness to pay or by exposing financial information through the payment process.

> there is no guarantee the perpetrator would not do it again. If I agree to pay money, I literally create more opportunities to reveal my personal information for perpetrator target me other times. (Respondent 2)

> if I paid them, I would be a target for other attacks since I assume they will post my details on the dark web and get other hackers to try target me as I will have a history of paying. (Respondent 14)

Some victims refused to pay the ransomware attackers out of principle and spoke about their desire to not fuel the ransomware business model, thereby potentially harming other victims in the process. These participants were angry and refused to give the cybercriminals the satisfaction of a successful attack.

> I was well aware that paying a ransom would only encourage and finance the criminals behind the attack. It would contribute to the perpetuation of these cybercrimes, potentially harming other victims in the process. Ethically, I couldn't justify supporting such criminal activities. (Respondent 16)

> I decided not to pay the ransom because I think it is really bad to compromise with this. If it happens to me, it may happen to anyone else. Lots of people will be the victims of ransom attacks. (Respondent 2)

A few victims spoke about the circumstances in which they would have paid, although only one respondent ultimately made the payment. One victim stated that he would have made the payment had he been in a financial position to do so. He was socially isolated, fearful of the offenders, and felt he had no way to resolve the situation.

> Honestly, I think if I had the money I would have paid. The experience was so scary and frightening that money did not seem to matter much. So I negotiated until he let me go … I convinced him that I'm really broke. (Respondent 32)

The one victim who paid was very distressed and confused about the incident, and indicated work-related files had been locked and money had been stolen. Despite a friend advising against payment, the victim ultimately paid the ransom.

> I am shocked for the first time, all my money is gone, I didn't understand what going around me … lost lot of information and legal staff and I need to retrieve it back… I informed my friend, he suggested me not to pay the ransom, I went against him and paid the ransom, I did not negotiate it. (Respondent 27)

Discussion

This study aimed to understand victim decision-making during a ransomware attack. It found victims consider a range of factors when assessing the threat and deciding how to respond and whether to pay the ransom. Our findings show that victims are capable of rational decision-making following ransomware attacks even during periods of heightened stress and emotion.

In assessing the validity of the claims made by ransomware attackers, victims gathered evidence and sought second opinions. They often expressed fear in response to receiving the messages, which had ominous tones and imagery and included personal information that the offenders claimed was proof they had hacked the victim. Despite this, victims were able to implement System 2 thinking processes, which involved calming themselves down, assessing evidence that their device had been compromised, and considering whether their personal information had been accessed in a ransomware attack or a third-party data breach. Victims who assessed the attack as serious and genuine considered several ways to respond. Victims were able to overcome feelings of fear, panic and self-blame despite the tactics used by the ransomware attackers. They found technical solutions, sought outside help and advice, and occasionally tried to negotiate a lower payment amount with the attackers.

The most important step was restoring their data and system functionality. Victims who were able to restore at least some of their stolen or encrypted data from backups and wipe the malware from their systems generally considered the situation resolved. This is consistent with Australian research finding that having backups is one of the most common reasons that ransomware victims give for not paying (Voce & Morgan 2021), although research from the Netherlands highlights that these backups must be recoverable (Meurs 2025). The importance of effective data backups must be central to ransomware prevention messaging.

Distrust in the attackers was commonly cited as a reason that victims did not communicate with the offenders, try to negotiate with them or decide to pay the ransom. In line with government advice (Australian Cyber Security Centre nd), victims knew that payment did not guarantee their systems and data would be restored and, furthermore, that paying may have put themselves at risk of being targeted again or put new victims at risk. In this way, victims did not view the decision as a simple transaction where they make a payment and their data and systems are restored, but as a gamble likely to result in further negative impacts (McIntyre & Frank 2021). While paying the ransom may seem, on the basis of limited information, the most rational decision (Connolly & Borrion 2022), the cost–benefit analysis by victims was shaped by outside information and their own moral judgement of what is right and wrong.

This study has important lessons that can help shape communication with and support for ransomware victims. Social support and publicly available information were both important in shaping victims' ability to assess the threat, understand what had occurred, find practical solutions, minimise the damage and decide whether to pay the ransom. Although ransomware actors usually warn the victim against telling anyone or seeking assistance from authorities (Matthijsse, Van 't Hoff-de Goede & Leukfeldt 2023), victims generally ignored these warnings. Research has shown that people are more likely to seek decision-making advice when they are fearful and when information about the outcome is lacking (Ferrer et al. 2022). This advice was key to shaping victims' decision-making and behaviour, which is consistent with previous research (Voce & Morgan 2022, 2021). Sources of advice included workplace IT support staff but also informal networks of trusted experts—such as friends and adult sons and daughters—who were not directly involved. These informal networks represent an important asset and finding ways to encourage these knowledgeable bystanders to intervene and support victims is a challenging but potentially valuable strategy, especially for victims in non-workplace settings and older victims (Nicholson et al. 2021).

Consistent with other studies, ransomware victims often did not make a formal report to police because they solved the problem themselves or with help from another party (Matthijsse, Van 't Hoff-de Goede & Leukfeldt 2025). However, some victims also explained that they did not know who could assist, felt responsible for the attack or believed the incident was not serious enough. These factors impede help-seeking by cybercrime victims more generally and can lead to official statistics that greatly underestimate the true extent of the problem (Voce & Morgan 2023). There is a need to raise awareness of government, law enforcement and non-government agencies which can offer non-judgemental assistance to ransomware victims during and after attacks.

Finally, knowing that people will be experiencing stress and negative emotion during a ransomware attack is important to consider when producing information for victims. Fear is well known to influence decision-making and how people assess and respond to risk (Wake, Wormwood & Satpute 2020). Stress also affects memory recall (Geißler et al. 2023), which is why information on what action to take must be close to hand. Having more information is positively associated with decision-making accuracy (Criado-Perez et al. 2024). Accurate, reliable and trustworthy resources to help victims assess the risks associated with a ransomware attack and act to restore their data and devices must be readily accessible to victims during a ransomware attack. It is especially important that this information be easily identifiable to victims during the midst of a ransomware attack, given the large amount of cyber safety information currently available online.

References

URLs correct as at February 2026

Angie AD, Connelly S, Waples EP & and Kligyte V 2011. The influence of discrete emotions on judgement and decision-making: A meta-analytic review. *Cognition and Emotion* 25(8): 1393–1422. https://doi.org/10.1080/02699931.2010.550751

Australian Cyber Security Centre nd. Report and recover from ransomware. https://www.cyber.gov.au/report-and-recover/recover-from/ransomware

Australian Signals Directorate 2024. *Annual cyber threat report 2023–2024*. Canberra: Australian Signals Directorate. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

Australian Signals Directorate nd. Ransomware. https://www.cyber.gov.au/threats/types-threats/ransomware

Bartholomeyczik K, Gusenbauer M & Treffers T 2022. The influence of incidental emotions on decision-making under risk and uncertainty: A systematic review and meta-analysis of experimental evidence. *Cognition and Emotion* 36(6): 1054–1073. https://doi.org/10.1080/02699931.2022.2099349

Connolly & Borrion 2022. Reducing ransomware crime: Analysis of victims' payment decisions. *Computers & Security* 119: 102760. https://doi.org/10.1016/j.cose.2022.102760

Cornish DB & Clarke RV 2014. *The reasoning criminal: Rational choice perspectives on offending*. New York: Routledge. https://doi.org/10.4324/9781315134482

Criado-Perez C, Jackson C, Minbashian A & Collins CG 2024. Cognitive reflection and decision-making accuracy: Examining their relation and boundary conditions in the context of evidence-based management. *Journal of Business and Psychology* 39: 249–273. https://doi.org/10.1007/s10869-023-09883-x

Ferrer RA, Ellis EM, Orehek E & Klein WMP 2022. Fear increases likelihood of seeking decisional support from others when making decisions involving ambiguity. *Journal of Behavioral Decision Making* 35(3): e2266. https://doi.org/10.1002/bdm.2266

Geißler CF, Friehs MA, Frings C & Domes G 2023. Time-dependent effects of acute stress on working memory performance: A systematic review and hypothesis. *Psychoneuroendocrinology* 148: 105998. https://doi.org/10.1016/j.psyneuen.2022.105998

Hull G, John H & Arief B 2019. Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science* 8(2). https://doi.org/10.1186/s40163-019-0097-9

Institute for Security and Technology 2021. *Combating ransomware: A comprehensive framework for action: Key recommendations from the Ransomware Task Force.* https://securityandtechnology.org/ransomwaretaskforce/

Kahneman D 2011. *Thinking, fast and slow*. New York: Farrar, Straus and Giroux

Kahneman D 2003. A perspective on judgement and choice. *American Psychologist* 58(9): 697–720. https://doi.org/10.1037/0003-066x.58.9.697

Matthijsse SR, Van 't Hoff-de Goede S & Leukfeldt ER 2025. To report or not to report: Exploring the motivations and factors associated with reporting of ransomware victimisation among entrepreneurs. *Journal of Criminal Justice* 97: 102378. https://doi.org/10.1016/j.jcrimjus.2025.102378

Matthijsse SR, Van 't Hoff-de Goede S & Leukfeldt ER 2023. Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-023-09496-z

McIntyre D & Frank R 2021. No gambles with information security: The victim psychology of a ransomware attack. In M Weulen Kranenbarg & R Leukfeldt (eds), *Cybercrime in context: The human factor in victimization, offending, and policing*. Cham: Springer: 43–60. https://doi.org/10.1007/978-3-030-60527-8_4

Meurs T 2025. *Double-extortion ransomware: A study of cybercriminal profit, effort, and risk* (doctoral thesis). University of Twente, Enschede, Netherlands. https://doi.org/10.3990/1.9789036564182

Nicholson J, Morrison B, Dixon M, Holt J, Coventry L & McGlasson J 2021. Training and embedding cybersecurity guardians in older communities. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. New York: Association for Computing Machinery: 1–15. https://doi.org/10.1145/3411764.3445078

Patyal M, Sampalli S, Qiang Y & Rahman M 2017. Multi-layered defense architecture against ransomware. *International Journal of Business and Cyber Security* 1. https://www.researchgate.net/publication/315471509_Multi-layered_defense_architecture_against_ransomware

Voce I & Morgan A 2025. Ransomware targeting individuals and small businesses: Vulnerabilities and impacts. *Trends & issues in crime and criminal justice* no. 724. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78106

Voce I & Morgan A 2023. *Cybercrime in Australia 2023*. Statistical Report no. 43. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr77031

Voce I & Morgan A 2022. *Help-seeking among Australian ransomware victims*. Statistical Bulletin no. 38. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78504

Voce I & Morgan A 2021. *Ransomware victimisation among Australian computer users*. Statistical Bulletin no. 35. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78382

Wake S, Wormwood J & Satpute AB 2020. The influence of fear on risk taking: A meta-analysis. *Cognition and Emotion* 34(6): 1143–1159. https://doi.org/10.1080/02699931.2020.1731428

Isabella Voce is a Principal Research Analyst in the Serious and Organised Crime, Cybercrime and Radicalisation Research Program at the Australian Institute of Criminology.

Anthony Morgan is Research Manager of the Serious and Organised Crime, Cybercrime and Radicalisation Research Program at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website: www.aic.gov.au

ISSN 1836-2206 (Online) ISBN 978 1 922878 29 8 (Online)

https://doi.org/10.52922/ti78298

GPO Box 1936
Canberra ACT 2601, Australia

Tel: 02 6268 7166

www.aic.gov.au