Australian Government
Australian Institute of Criminology

# Statistical Bulletin 40

November 2022

**Abstract |** This paper draws on data from a large national survey conducted in 2021 to examine the prevalence of data breaches among Australian computer users and the relationship between data breaches and other forms of cybercrime victimisation.

Almost one in 10 respondents (9.3%) said they were notified their information was exposed in a data breach in the 12 months prior to the survey. Nearly one-third of these respondents (28.0%) had also been a victim of identity crime in the same period. Respondents who had been notified of a data breach were 34 percent more likely than other respondents to have been a victim of identity crime in the 12 months prior to the survey. They were also more likely to have been a victim of online scams or fraud and ransomware.

Measures to protect individuals whose information has been exposed in a data breach from other potentially related cybercrimes are essential and should be prioritised when data breaches occur.

## Data breaches and cybercrime victimisation

Anthony Morgan and Isabella Voce

Recent high-profile data breaches have drawn attention to the risks that the release of personal information poses to individuals and businesses. Large-scale breaches can affect millions of customers, as was illustrated in the recent breaches of data held by telecommunications company Optus and health insurance provider Medibank (ABC News 2022; Terzon 2022). When this information is made available to malicious actors, it can be used in myriad ways to steal a person's identity or target vulnerable computer users, ultimately allowing opportunistic offenders to generate profit.

Data breaches are not always caused by a malicious actor. According to the Office of the Australian Information Commissioner (2022), half of the notifiable data breaches (55%) in the most recent reporting period were due to a malicious or criminal attack, while 41 percent were the result of human error, such as personal information being unintentionally published or sent to the wrong recipient. Certain sectors are more vulnerable than others, with health service providers the most frequently targeted (Office of the Australian Information Commissioner 2022).

Serious & Organised Crime Research Laboratory

Information exposed in data breaches can be used by motivated and opportunistic offenders to gain access to the secure accounts of individuals and businesses. This information can be used to commit other related crimes, particularly those crimes that immediately benefit from access to personally identifying information. According to McAlister and Franks (2021), 12 percent of victims of identity crime and misuse of personal information—which they define as obtaining or using personal information to carry out a business, other types of activities and transactions in a person's name without their permission—said that their personal information had been obtained via a data breach.

Offenders can also use information from data breaches to create targeted campaigns that have an increased likelihood of success (Europol 2021). There is, as a result, a growing market for personal information obtained through data breaches (Holt, Smirnova & Chua 2016), particularly on the darknet (Smirnova & Holt 2017). Data breaches have also been closely linked to ransomware attacks (Australian Cyber Security Centre 2021; Europol 2021).

In this study, we explore how common it was among a large sample of Australian computer users to have been notified that their information had been exposed in a data breach. We then examine the prevalence of self-reported cybercrime victimisation among computer users who reported being notified of a data breach and measure the relationship between data breaches and cybercrime victimisation.

# Method

## Data

This study uses data collected as part of the Australian Institute of Criminology's pilot Australian Cybercrime Survey, conducted in mid-2021. This survey asked 15,000 members of the public about a range of experiences related to cybercrime victimisation. Invitations were sent to 171,537 individual members of an established online research panel. Non-proportional quota-based sampling—with quotas for age, gender and state/territory—was used to ensure the sample was representative of the Australian population. The survey had an overall completion rate of nine percent, but 76.8% of respondents who accessed the survey and read the information sheet went on to complete it. Post-stratification weights were applied to male and female respondents using demographic data as of December 2020 (Australian Bureau of Statistics 2021). Six respondents were removed from the sample due to data quality issues detected during data cleaning, resulting in a final survey sample of 14,994 respondents. Further information is provided in the *Method* section of Voce and Morgan (2021).

The survey included a question about whether the respondent had been notified that their information had been exposed in a data breach in the 12 months prior to the survey. While we acknowledge that other respondents may have fallen victim to a data breach, whether due to a malicious actor or human error, we wanted to identify those respondents who had been specifically notified of a breach. This distinguishes them from respondents who assumed they had been a victim of a data breach because they had experienced some form of cybercrime that compromised their identity.

The survey adopted a bottom-up approach to measuring cybercrime victimisation, given the difficulties respondents may have in accurately identifying whether they had been a victim, and the broad range of criminal activities that fall under the definition of cybercrime (Phillips et al. 2022). The survey included several items that were used to measure whether respondents had ever:

- been a victim of identity theft, compromise or misuse (excluding data breaches)—hereafter referred to as identity crime;
- been a victim of an online scam or fraud; or
- received instructions on their device for paying a ransom—hereafter referred to as ransomware.

This approach enabled us to measure overall rates of victimisation for the major categories of cybercrime (ie identity crime, online scams or fraud, and ransomware) as well as for specific indicators or subtypes of these cybercrimes.

## Analysis

We began by examining simple descriptive statistics for the overall prevalence of data breaches and the relationship between data breaches and key socio-demographic characteristics and computer activity. This was followed by an analysis of cybercrime victimisation (including identity crime, online scams and fraud, and ransomware) among respondents who were notified their information had been exposed in a data breach.

We then compared respondents who had and had not been notified that their information had been exposed in a data breach in terms of whether they had also been a victim of identity crime, online scams and fraud, or ransomware. We could not compare the two groups based on raw prevalence rates, because there may be important differences between respondents who had and had not been notified of a data breach that are associated with the likelihood of being a victim of cybercrime. For each type (and subtype) of cybercrime, we estimated a logistic regression model to measure the relationship between being notified of a data breach and being a cybercrime victim in the 12 months prior to the survey, while controlling for the potential confounding effect of other variables in the model.

We drew on prior research on demographic characteristics and routine online activities associated with cybercrime victimisation (Holt et al. 2020; Leukfeldt & Yar 2016). Each model included variables relating to key socio-demographic characteristics, including the respondents' age, gender, employment status, language spoken at home, restrictive health conditions, and whether they had children at home. The models also included variables relating to computer use and activity, including:

- the average number of hours spent per day using the internet for personal use;
- the frequent use of platforms that might be regarded as vulnerable to exploitation (such as online marketplaces, dating websites, sexually explicit websites and gaming platforms);
- the use of practices which might increase the likelihood of personal information being accessible to malicious actors; and
- respondents' self-rated ability to use digital technologies.

The analysis was undertaken using weighted data.

We were primarily interested in whether having been notified of a data breach was a statistically significant factor once these other variables had been taken into account, meaning we can be confident data breach notifications were associated with a change in the likelihood of victimisation. We calculated adjusted odds ratios, which measure the strength of this relationship. We then determined the marginal effect of a respondent's information being exposed in a data breach, which indicates how much the probability of victimisation changes, controlling for other variables. This is based on average predictive margins estimated using the marginal standardisation method (Muller & MacLehose 2014).

The prevalence of each indicator of identity crime was relatively low among the sample, with all but two indicators falling below five percent. The same was true of the prevalence of ransomware victimisation. By way of a robustness check, we used rare event logistic regression to re-estimate the model for each indicator and for ransomware victimisation (King & Zeng 2001). Results from these rare event models are presented in Table A1 in the *Appendix* and confirm the results from the logistic regression models presented below.

## Limitations

Limitations associated with the survey methodology more broadly and with the analysis presented in this paper should be acknowledged. The benefit of online panels is that they allow for the collection of data from large samples, particularly when the main population of interest is computer users. The sample in this study is large and representative of the spread of the Australian population, but it is a non-probability sample and we must be cautious about generalising beyond the survey respondents.

A large proportion of respondents declined to answer the questions about whether they were a victim of different forms of cybercrime. This could be for a range of reasons, including shame or embarrassment, which is a common emotion among victims of cybercrime (Cross, Richards & Smith 2016), or because they were uncertain whether they had been a victim. Because there is a high likelihood of non-response being correlated with the outcome (ie people who were victims being less likely to respond), we relied on casewise deletion. While these accounted for most missing data in the sample, a smaller proportion of cases were missing data on key socio-demographic characteristics and computer activity. Overall, around 10 percent of cases were excluded due to missing data, and we acknowledge that this may have a small effect on the robustness of the results.

Of particular relevance to this study is that not everyone who has been a victim of a data breach will be aware that their personal information has been exposed, meaning the prevalence of data breaches reported in this study is almost certainly an underestimate. In many instances, a person will need to be notified by the custodian of the data accessed, or another service provider who becomes aware of the breach, potentially as a consequence of an individual falling victim to another type of cybercrime. It is possible that some respondents were made aware of their information being exposed in a data breach because they fell victim to another type of cybercrime. This may explain some of the observed differences. However, most victims did not report having had their information exposed in a data breach, and this does not vary significantly between the different subtypes of identity crime (identity theft, compromise and misuse), suggesting any effect is small. We were able to address this limitation by separately considering the results for the different subtypes of identity crime, including those in which it is unlikely that a data breach would be automatically assumed to be the cause (such as finding suspicious transactions on your credit card).

Finally, the study uses cross-sectional data, meaning that we could not establish with certainty whether cybercrime victimisation occurred before or after the respondents were notified of a data breach. We therefore focused solely on the association between data breaches and cybercrime victimisation.

# Results

## Prevalence of data breaches

Overall, 9.3 percent of survey respondents said they had been notified that their information was exposed in a data breach in the 12 months prior to the survey. The proportion of survey respondents who had received such a notification varied according to socio-demographic characteristics (Table 1). Male respondents were more likely than female respondents to have been notified of a data breach (10.2% vs 8.4%, $F$=14.3, $p$<0.001), while respondents aged 18 to 34 years (10.4%) and 35 to 64 years (9.8%) were more likely than respondents aged 65 years and over (6.5%) to have been notified their information was exposed ($F$=17.6, $p$<0.001). There was a significant relationship between employment status and data breaches, with respondents who were not currently working (7.0%) less likely than any other employment category to have had their information exposed in a data breach ($F$=16.8, $p$<0.001). Finally, respondents who said they had a restrictive long-term health condition were also more likely than other respondents to have been notified of a data breach in the 12 months prior to the survey (11.2% vs 9.2%, $F$=4.5, $p$<0.05). Some of these differences may be explained by differences in online behaviour between groups.

Many data breaches occur when data custodians are targeted by a malicious actor or information held by these data custodians is released due to human error. However, certain internet practices appear to make individuals more vulnerable to having their information exposed in a data breach. This includes daily or weekly use of platforms that might be regarded as more vulnerable to exploitation, such as online marketplaces, dating websites, sexually explicit websites and gaming platforms. Among survey respondents who used such platforms frequently, 11.7 percent had been notified of a data breach, compared with 6.7 percent of those who used these platforms less often or never ($F$=100.8, $p$<0.001).

Certain practices might also increase the likelihood of personal information being accessible to malicious actors, such as using public wi-fi, sharing account passwords with someone else, or opening emails from unknown people or organisations. Respondents who engaged in these unsafe online activities were more likely than other respondents to report having their information exposed in a data breach (14.5% vs 7.5%, $F$=153.2, $p$<0.001).

While there was no relationship between the average number of hours people used the internet for personal use and data breaches (4.1 hours among respondents who were notified of a data breach vs 4.1 hours among respondents who were not, $t$= −0.8, $p$=0.44), the average number of hours respondents used a digital device for work was positively associated with the likelihood of being notified of a data breach (5.1 hours vs 4.6 hours, $t$= −3.7, $p$<0.001). Further, respondents' self-rated ability to use digital devices was significantly associated with the likelihood of a data breach ($F$=67.4, $p$<0.001); however, data breaches were more common among those who rated their ability as high or very high (12.9%) or moderate (8.2%) than among respondents who said it was low or very low (4.5%).

**Table 1: Survey respondents who had been notified that their information had been exposed in a data breach, by selected demographic characteristics and computer activity (*n*=14,994)**

| | *n* | % | |
|---|---|---|---|
| **Gender**[a] | | | |
| Male | 7,326 | 10.2 | *F*=14.3, *p*<0.001[b] |
| Female | 7,610 | 8.4 | |
| Non-binary | 39 | 12.8 | |
| **Age** | | | |
| 18–34 years | 4,614 | 10.4 | *F*=17.6, *p*<0.001 |
| 35–64 years | 7,246 | 9.8 | |
| 65 years and over | 3,134 | 6.5 | |
| **Employment status**[c] | | | |
| Small to medium enterprise (SME) owner | 2,166 | 10.9 | *F*=16.8, *p*<0.001 |
| SME employee | 2,819 | 9.6 | |
| Employed (but not owner or employee of SME) | 4,719 | 10.9 | |
| Not currently working | 4,989 | 7.0 | |
| **Restrictive long-term health condition**[d] | | | |
| Yes | 1,195 | 11.2 | *F*=4.5, *p*<0.05 |
| No | 13,396 | 9.2 | |
| **Speaks a language other than English at home**[e] | | | |
| Yes | 1,085 | 7.9 | *F*=2.3, *p*=0.13 |
| No | 13,855 | 9.4 | |
| **Uses high-risk platforms on a daily or weekly basis**[f] | | | |
| Yes | 7,954 | 11.7 | *F*=100.8, *p*<0.001 |
| No | 6,790 | 6.7 | |
| **Unsafe online activities** | | | |
| Yes | 3,758 | 14.5 | *F*=153.2, *p*<0.001 |
| No | 11,236 | 7.5 | |
| **Self-rated digital ability**[g] | | | |
| Low or very low | 2,055 | 4.5 | *F*=67.4, *p*<0.001 |
| Moderate | 7,197 | 8.2 | |
| High or very high | 5,536 | 12.9 | |

a: 19 respondents did not provide this information

b: 39 non-binary respondents excluded due to small cell size

c: 300 respondents did not provide this information. Not currently working includes respondents who were currently unemployed (7.9%); who were studying, a full time homemaker or in other circumstances (7.0%); or who were retired or on a pension (6.8%)

d: 403 respondents did not provide this information

e: 54 respondents did not provide this information

f: 250 respondents did not provide this information

g: 207 respondents did not provide this information

Source: Australian Cybercrime Survey 2021 [weighted data]

## Cybercrime victimisation among respondents notified of a data breach

Nearly a third of respondents (28.0%) who said they had been notified of a data breach also reported some evidence of having been a victim of identity crime in the previous 12 months (Table 2). This most frequently involved evidence of suspicious financial transactions. One in 10 respondents (11.0%) had been notified by a financial institution that their identity had been stolen or that there was suspicious activity on their account. Further, 8.3 percent said unfamiliar and unauthorised activity had appeared on their credit card, 8.1 percent were contacted about unpaid bills they did not recognise, and 6.0 percent said that suspicious transactions had appeared on their bank statement. A smaller proportion said they had received goods (2.3%) or credit cards (1.4%) in the mail they had not ordered or applied for, while evidence that utilities (1.5%) or medical accounts (1.3%) had been corrupted was also relatively uncommon.

In terms of other types of cybercrime, 12.7 percent of respondents who said they had been notified their information had been exposed in a data breach said they had also been a victim of an online scam or fraud in the 12 months prior to the survey. In addition, 4.1 percent of respondents who said they had been notified of a data breach said they had also been a victim of ransomware in the 12 months prior to the survey.

**Table 2: Indicators of identity crime experienced by respondents whose information was exposed in a data breach (*n*=1,393)**

| | *n* | % |
|---|---|---|
| They were notified by a bank, financial institution or credit card company that their identity had been stolen or that there was suspicious, unrecognised activity on their account | 154 | 11.0 |
| Unfamiliar and unauthorised activity appeared on their credit card or credit report | 116 | 8.3 |
| They received calls from debt collectors asking about unpaid bills they didn't recognise | 113 | 8.1 |
| Suspicious transactions appeared in their bank statements or accounts, or their cheques bounced | 84 | 6.0 |
| They were unsuccessful in applying for credit and this was surprising given their credit history | 38 | 2.7 |
| They were notified by the police or a government agency that their identity had been stolen | 35 | 2.5 |
| Their bills were missing or they received unfamiliar bills | 32 | 2.3 |
| They received goods in the mail, such as mobile phones, that they did not order | 32 | 2.3 |
| Their mobile phone or other utility lost service because their service had been transferred to a new unknown device | 22 | 1.5 |
| They received credit or payment cards in the mail that they did not apply for | 20 | 1.4 |
| They got a medical bill for a service they didn't receive, or their medical claim was rejected because they had unexpectedly reached their benefits limit | 19 | 1.3 |
| They were unable to file taxes because someone had already filed a tax return in their name | 12 | 0.9 |
| Any evidence of identity theft, compromise or misuse | 390 | 28.0 |

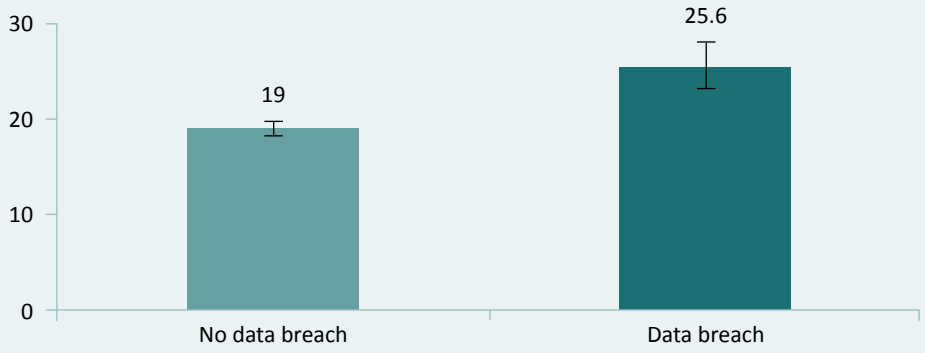
Note: Respondents could select multiple indicators of identity crime
Source: Australian Cybercrime Survey 2021 [weighted data]

## Relationship between data breaches and cybercrime victimisation

### *Identity crime*

We used logistic regression models to measure the relationship between having been notified of a data breach and different forms of cybercrime, starting with the overall prevalence of identity crime, while controlling for socio-demographic characteristics and online behaviour. There was a statistically significant relationship between being notified of a data breach and being a victim of identity crime (AOR=1.9, 95% CI [1.3, 1.7], $p<0.001$). After adjusting for key differences between the two groups, respondents who received notification of a data breach were 34.4 percent more likely to have been a victim of identity crime than respondents who had not been notified of a data breach (25.6% vs 19.0%).

**Figure 1: Estimated probability of identity crime victimisation, by whether respondent was notified of a data breach (%) (*n*=13,528)**




*F*=40.97, $p<0.001$, AUROC=0.653; AME=0.07, $t$=5.19, $p<0.01$

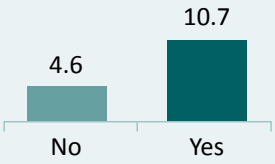
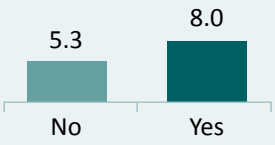
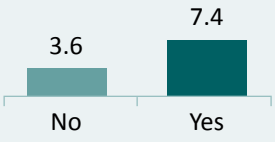
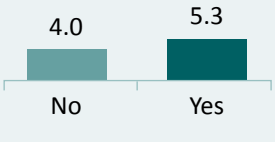
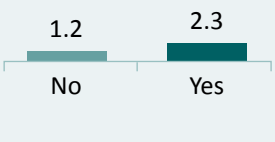
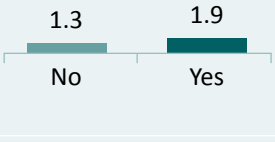
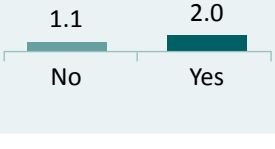
Note: Estimated probabilities are derived from predicted margins from logistic regression using weighted data. Error bars represent 95% confidence interval for estimated probability

Source: Australian Cybercrime Survey 2021 [weighted data]

We then repeated this analysis for individual indicators of identity crime. This enabled us to identify whether specific types of victimisation were more likely among respondents whose information was exposed in a data breach. Respondents whose information was exposed in a data breach were 130.6 percent more likely than other respondents to be notified by a bank, financial institution or credit card company that their identity had been stolen or that there was suspicious, unrecognised activity on their account (10.7% vs 4.6%). Given that respondents may have conflated a data breach notification with a notification from a financial institution about identity theft, this may not be the best indicator of the effect of data breaches on cybercrime risk.

Further analysis reveals a significant relationship between data breaches and a number of other subtypes or indicators of identity crime. Respondents who were notified their information was exposed in a data breach were 50.0 percent more likely to also report unfamiliar and unauthorised activity on their credit card (8.0% vs 5.3%), 103.9% more likely to receive calls about unpaid bills (7.4% vs 3.6%), and 34.2 percent more likely to report suspicious transactions in their bank statements or accounts (5.3% vs 4.0%). Though much less common among respondents, those who were notified of a data breach were also 101.3 percent more likely to be unsuccessful in applying for credit (2.3% vs 1.2%), 80.7 percent more likely to report missing or unfamiliar bills (2.0% vs 1.1%), and 109.2 percent more likely to receive goods in the mail they did not order (2.0% vs 1.0%).

**Table 3: Indicators of identity crime experienced by respondents whose information was exposed in a data breach (*n*=13,528)**

| | AOR (95% CI) | Probability of victimisation by whether notified of data breach | % diff. (pp) |
|---|---|---|---|
| They were notified by a bank, financial institution or credit card company that their identity had been stolen or that there was suspicious, unrecognised activity on their account | 2.5***<br>(2.0, 3.1) |  | +130.6<br>(6.1) |
| Unfamiliar and unauthorised activity appeared on their credit card or credit report | 1.54***<br>(1.25, 1.92) |  | +50.0<br>(2.7) |
| They received calls from debt collectors asking about unpaid bills they didn't recognise | 2.1***<br>(1.7, 2.7) |  | +103.9<br>(3.7) |
| Suspicious transactions appeared in their bank statements or accounts, or their cheques bounced | 1.4*<br>(1.1, 1.8) |  | +34.2<br>(1.4) |
| They were unsuccessful in applying for credit and this was surprising given their credit history | 2.1***<br>(1.4, 3.1) |  | +101.3<br>(1.2) |
| They were notified by the police or a government agency that their identity had been stolen[a] | 1.5<br>(1.0, 2.2) |  | – |
| Their bills were missing or they received unfamiliar bills | 1.9**<br>(1.2, 2.9) |  | +80.7<br>(0.9) |

| Table 3: Indicators of identity crime experienced by respondents whose information was exposed in a data breach (*n*=13,528) | | | |
|---|---|---|---|
| They received goods in the mail, such as mobile phones, that they did not order | 2.2**<br>(1.4, 3.4) |  | +109.2<br>(1.0) |
| Their mobile phone or other utility lost service because their service had been transferred to a new unknown device | 1.2<br>(0.7, 2.0) |  | – |
| They received credit or payment cards in the mail that they did not apply for | 1.4<br>(0.8, 2.4) |  | – |
| They got a medical bill for a service they didn't receive, or their medical claim was rejected because they had unexpectedly reached their benefits limit | 1.1<br>(0.6, 1.8) |  | – |
| They were unable to file taxes because someone had already filed a tax return in their name | 1.1<br>(0.5, 2.1) |  | – |

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

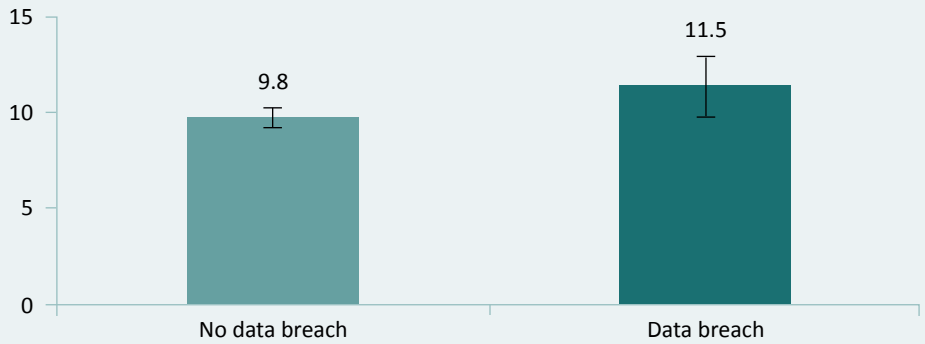
a: The coefficient for this indicator was significant in the rare events logistic regression (see Table A1). We opted to present results from the original logistic regression model for consistency and because it represents a more conservative estimate

Note: AOR=adjusted odds ratio, CI=confidence intervals, pp=percentage point. Estimated probabilities are derived from predicted margins from logistic regression using weighted data and including controls for demographic characteristics and computer activity and security

## *Online scams and fraud*

There was a statistically significant relationship between being notified of a data breach and being a victim of an online scam or fraud (AOR=1.2, 95% CI [1.0, 1.5], $p<0.05$). After adjusting for key differences between the two groups, respondents who were notified of a data breach were 16.8 percent more likely to have been a victim of an online scam or fraud than respondents who had not been notified of a data breach (11.5% vs 9.8%).

**Figure 2: Estimated probability of online scam or fraud victimisation, by whether respondent was notified their information was exposed in a data breach (%) (*n*=13,362)**




*F*=56.70, *p*<0.001, AUROC=0.760; AME=0.02, *t*=1.93, *p*=0.05

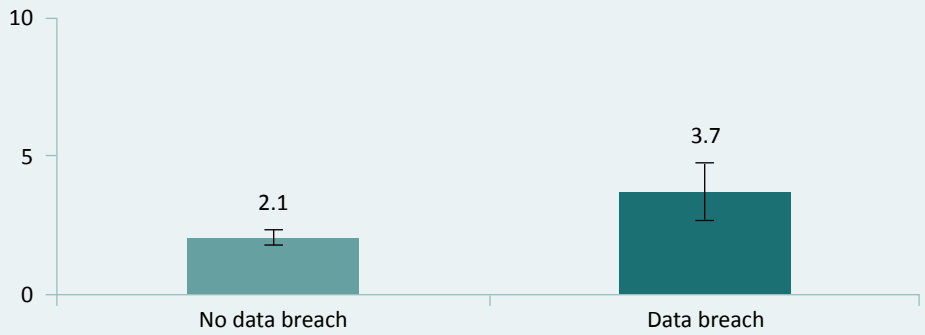
Note: Estimated probabilities are derived from predicted margins from logistic regression using weighted data and including controls for demographic characteristics and computer activity and security

Source: Australian Cybercrime Survey 2021 [weighted data]

### *Ransomware*

Alongside other questions about malware victimisation, respondents were asked whether they had received instructions on their device for paying a ransom (see Voce & Morgan 2021 for a more detailed discussion of ransomware victimisation). There was a statistically significant relationship between being notified of a data breach and being a victim of ransomware in the 12 months prior to the survey (AOR=1.8, 95% CI [1.3, 2.6], $p<0.001$). Respondents who had been notified of a data breach were 79.5 percent more likely to have also received a ransom message on their device. This is equivalent to an increase in the estimated probability of being a ransomware victim from 2.1 percent to 3.7 percent.

**Figure 3: Estimated probability of ransomware victimisation, by whether respondent was notified their information was exposed in a data breach (%) (*n*=13,046)**




*F*=11.77, *p*<0.001, AUROC=0.706; AME=0.02, *t*=3.00, *p*<0.01

Note: Estimated probabilities are derived from predicted margins from logistic regression using weighted data and including controls for demographic characteristics and computer activity and security

Source: Australian Cybercrime Survey 2021 [weighted data]

## Discussion

Recent events have focused attention on the potential risks that large-scale data breaches present, particularly as they expose individuals to cybercrime victimisation. This paper draws on data collected in 2021 from a large sample of Australian computer users to explore the relationship between being notified of a data breach and being a victim of different types of cybercrime—specifically, the forms of cybercrime that require or benefit from access to the personal information of prospective victims.

Almost one in 10 respondents (9.3%) said they were notified their information was exposed in a data breach in the last 12 months. Data breaches were more common among certain groups, including younger respondents, men, and respondents with a restrictive long-term health condition. People who were working were more likely to report having been notified of a data breach. Among those who were working, the likelihood of data breaches was higher among respondents who spent more time online for work. While many data breaches target organisations rather than individuals, using more vulnerable websites or platforms and engaging in practices known to undermine cyber safety were both associated with a higher likelihood of data breaches. Counterintuitively, those respondents who rated their digital ability more highly were more likely to say their information was exposed in a data breach. This suggests that online activity may have a greater influence on the likelihood of having personal information exposed in a data breach than digital knowledge or ability. Indeed, the likelihood of having your personal information exposed in a data breach is a function of the data custodians with which your personal information is shared, their vulnerability to malicious actors and their capacity to avoid human error.

A significant proportion of respondents who had been notified their information was exposed in a data breach in the last 12 months were also victims of cybercrime. Nearly a third of respondents who said they had been notified of a data breach also reported some evidence of having been a victim of identity crime in the previous 12 months. This most frequently involved evidence of suspicious financial transactions—being notified by a financial institution that their identity had been stolen, unauthorised activity appearing on their credit card, being contacted about unpaid bills, and suspicious transactions appearing on their bank statement. The misuse of personal information for direct financial gain is a common feature of identity crime (McAlister & Franks 2021).

Overall, once key demographic characteristics and computer activity were taken into account, the estimated probability of identity crime victimisation was 34 percent higher for respondents who were notified that their personal information had been exposed in a data breach. There was a smaller increase in the likelihood of being a victim of online scams or fraud (which is less common overall than identity crime). This may be because access to personal information is not sufficient to carry out an online fraud or scam. Rather, it enables motivated offenders to better target potential victims, without necessarily increasing their likelihood of success. People whose information was exposed in a data breach were also nearly twice as likely as other respondents to have been a victim of ransomware. Ransomware messages may include threats to release data that have already been exposed in a data breach (meaning respondents became aware of the data breach because they were a victim of ransomware); however, extortion without encryption accounts for only a very small proportion of ransomware attacks (Sophos 2022). We note the limitations of not being able to link directly the data breach and other types of cybercrime, but there is clear evidence that people who are notified that their information has been exposed in a data breach are more likely to be a victim of cybercrime, particularly forms of cybercrime that involve the malicious use of personal information.

# References

*URLs correct as at October 2022*

ABC News 2022. Optus reveals more than 2 million customers had personal ID numbers compromised in cyber attack. *ABC News*, 3 October. https://www.abc.net.au/news/2022-10-03/optus-data-breach-cyber-attack-deloitte-review-audit/101496190

Australian Bureau of Statistics (ABS) 2021. *Population by age and sex - national. National, state and territory population, Dec 2020*. https://www.abs.gov.au/statistics/people/population/national-state-and-territory-population/dec-2020#data-downloads-data-cubes

Australian Cyber Security Centre (ACSC) 2021. *ACSC annual cyber threat report: 1 July 2020 to 30 June 2021*. Canberra: ACSC. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2020-june-2021

Cross C, Richards K & Smith RG 2016. The reporting experiences and support needs of victims of online fraud. *Trends & issues in crime and criminal justice* no. 518. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi518

Europol 2021. *Internet organised crime threat assessment (IOCTA) 2021*. Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Holt TJ, Smirnova O & Chua YT 2016. Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior* 37(4): 353–367. https://doi.org/10.1080/01639625.2015.1026766

Holt TJ, van Wilsem J, van de Weijer S & Leukfeldt R 2020. Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review* 38(2): 187–206. https://doi.org/10.1177/0894439318805067

King G & Zeng L 2001. Logistic regression in rare events data. *Political Analysis* 9(2): 137–163. https://doi.org/10.1093/oxfordjournals.pan.a004868

Leukfeldt ER & Yar M 2016. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior* 37(3): 263–280. https://doi.org/10.1080/01639625.2015.1012409

McAlister M & Franks C 2021. *Identity crime and misuse in Australia: Results of the 2021 online survey*. Statistical Bulletin no. 37. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78467

Muller CJ & MacLehose RF 2014. Estimating predicted probabilities from logistic regression: Different methods correspond to different target populations. *International Journal of Epidemiology* 43(3): 962–970. https://doi.org/10.1093/ije/dyu029

Office of the Australian Information Commissioner (OAIC) 2022. *Notifiable data breaches report: July–December 2021*. Canberra: OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021

Phillips K, Davidson JC, Farr RR, Burkhardt C, Caneppele S & Aiken MP 2022. Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Science* 2: 379–398. https://doi.org/10.3390/forensicsci2020028

Smirnova O & Holt TJ 2017. Examining the geographic distribution of victim nations in stolen data markets. *American Behavioral Scientist* 61(11): 1403–1426. https://doi.org/10.1177/0002764217734270

Sophos 2022. The state of ransomware 2022. https://www.sophos.com/en-us/content/state-of-ransomware

Terzon E 2022. Medibank reveals customer data breach much wider than originally thought. *ABC News*, 25 October. https://www.abc.net.au/news/2022-10-25/medibank-breach-wider-than-estimated/101572904

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

# Appendix

**Table A1: Rare events logistic regression estimating likelihood of being a victim of different types of cybercrime**

| | B | 95% CIs |
|---|---|---|
| **Identity crime (*n*=13,556)** | | |
| They were notified by a bank, financial institution or credit card company that their identity had been stolen or that there was suspicious, unrecognised activity on their account | 0.91*** | 0.71, 1.10 |
| Unfamiliar and unauthorised activity appeared on their credit card or credit report | 0.39*** | 0.18, 0.60 |
| They received calls from debt collectors asking about unpaid bills they didn't recognise | 0.76*** | 0.54, 0.98 |
| Suspicious transactions appeared in their bank statements or accounts, or their cheques bounced | 0.32* | 0.08, 0.58 |
| They were unsuccessful in applying for credit and this was surprising given their credit history | 0.83*** | 0.45, 1.21 |
| They were notified by the police or a government agency that their identity had been stolen | 0.45* | 0.03, 0.86 |
| Their bills were missing or they received unfamiliar bills | 0.57** | 0.14, 0.99 |
| They received goods in the mail, such as mobile phones, that they did not order | 0.74** | 0.31, 1.16 |
| Their mobile phone or other utility lost service because their service had been transferred to a new unknown device | 0.26 | −0.23, 0.75 |
| They received credit or payment cards in the mail that they did not apply for | 0.37 | −0.13, 0.88 |
| They got a medical bill for a service they didn't receive, or their medical claim was rejected because they had unexpectedly reached their benefits limit | 0.09 | −0.45, 0.63 |
| They were unable to file taxes because someone had already filed a tax return in their name | 0.10 | −0.57, 0.76 |
| **Ransomware (*n*=13,081)** | | |
| They received instructions on their device for paying a ransom | 0.55** | 0.24, 0.87 |

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$
Note: CIs=confidence intervals. Results are based on rare events logistic regression using unweighted data
Source: Australian Cybercrime Survey 2021

**Anthony Morgan is the Research Manager of the Australian Institute of Criminology's Serious and Organised Crime Research Laboratory.**

**Isabella Voce is a Senior Research Analyst in the Australian Institute of Criminology's Serious and Organised Crime Research Laboratory.**

General editor, Statistical Bulletin series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology.
For a complete list and the full text of the papers in the Statistical Bulletin series, visit the AIC website at: aic.gov.au

ISSN 2206-7302 (Online)
ISBN 978 1 922478 83 2 (Online)
https://doi.org/10.52922/sb78832



GPO Box 1936
Canberra ACT 2601, Australia
Tel: 02 6268 7166