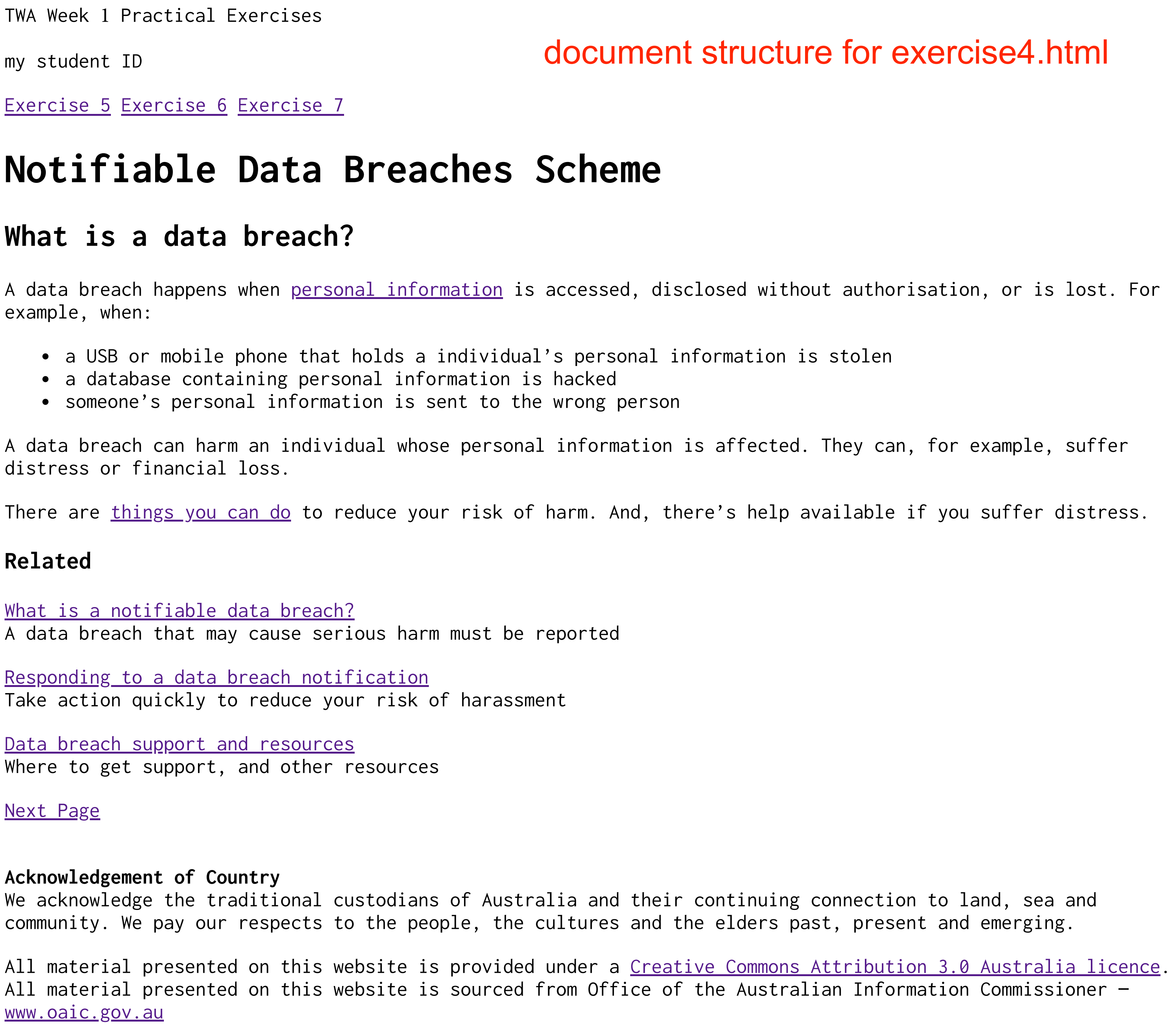
document structure for exercise4.html



TWA Week 1 Practical Exercises

my student ID

Exercise 5 Exercise 6 Exercise 7

Notifiable Data Breaches Scheme

What is a data breach?

A data breach happens when personal information is accessed, disclosed without authorisation, or is lost. For example, when:

- a USB or mobile phone that holds a individual's personal information is stolen
- a database containing personal information is hacked
- someone's personal information is sent to the wrong person

A data breach can harm an individual whose personal information is affected. They can, for example, suffer distress or financial loss.

There are things you can do to reduce your risk of harm. And, there's help available if you suffer distress.

Related

What is a notifiable data breach?
A data breach that may cause serious harm must be reported

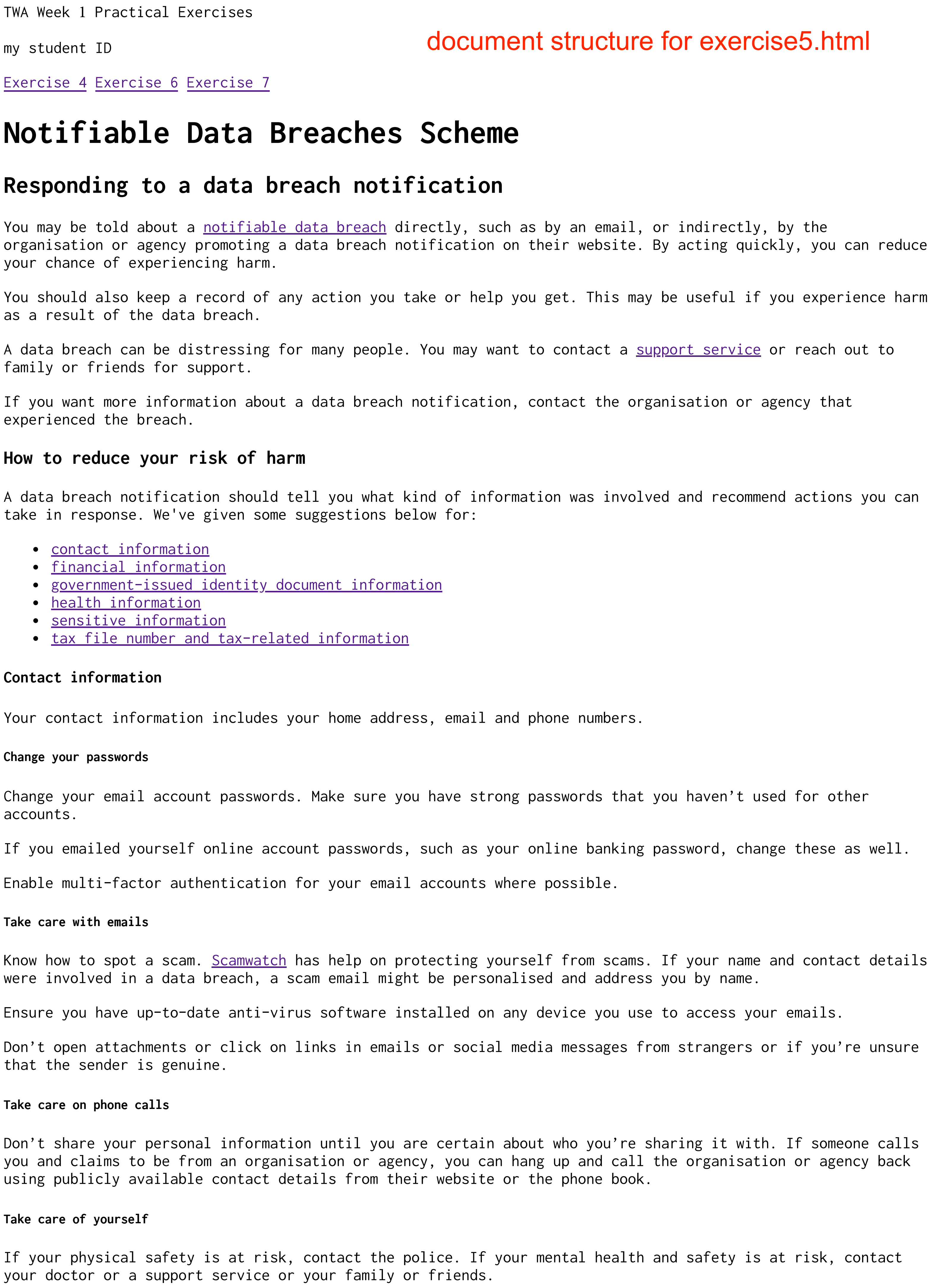
Responding to a data breach notification
Take action quickly to reduce your risk of harassment

Data breach support and resources
Where to get support, and other resources

Next Page

Acknowledgement of Country
We acknowledge the traditional custodians of Australia and their continuing connection to land, sea and community. We pay our respects to the people, the cultures and the elders past, present and emerging.

document structure for exercise5.html



TWA Week 1 Practical Exercises

my student ID

Exercise 4 Exercise 6 Exercise 7

Notifiable Data Breaches Scheme

Responding to a data breach notification

You may be told about a notifiable data breach directly, such as by an email, or indirectly, by the organisation or agency promoting a data breach notification on their website. By acting quickly, you can reduce your chance of experiencing harm.

You should also keep a record of any action you take or help you get. This may be useful if you experience harm as a result of the data breach.

A data breach can be distressing for many people. You may want to contact a support service or reach out to family or friends for support.

If you want more information about a data breach notification, contact the organisation or agency that experienced the breach.

How to reduce your risk of harm

A data breach notification should tell you what kind of information was involved and recommend actions you can take in response. We've given some suggestions below for:

- contact information
- financial information
- government-issued identity document information
- health information
- sensitive information
- tax file number and tax-related information

Contact information

Your contact information includes your home address, email and phone numbers.

Change your passwords

Change your email account passwords. Make sure you have strong passwords that you haven’t used for other accounts.

If you emailed yourself online account passwords, such as your online banking password, change these as well.

Enable multi-factor authentication for your email accounts where possible.

Take care with emails

Know how to spot a scam. Scamwatch has help on protecting yourself from scams. If your name and contact details were involved in a data breach, a scam email might be personalised and address you by name.

Ensure you have up-to-date anti-virus software installed on any device you use to access your emails.

Don’t open attachments or click on links in emails or social media messages from strangers or if you’re unsure that the sender is genuine.

Take care on phone calls

Don’t share your personal information until you are certain about who you’re sharing it with. If someone calls you and claims to be from an organisation or agency, you can hang up and call the organisation or agency back using publicly available contact details from their website or the phone book.

Take care of yourself

If your physical safety is at risk, contact the police. If your mental health and safety is at risk, contact your doctor or a support service or your family or friends.

Financial information

If you have any questions about financial information (such as your credit card details or online banking sign in) that a data breach notification doesn’t answer, contact your financial institution using the contact details on their website or in the phone book.

Change your passwords

Change your online banking account passwords. Use a strong password that you’ve not used for other accounts. Also, change your banking PIN number.

When updating your internet banking passwords, go to the financial institution’s website directly by typing their web address into your web browser. Generally, a financial institution won’t ask you in an email to click on a link to update your password.

You might also consider enabling multi-factor authentication for your accounts if it’s available. Multi-factor authentication asks you to confirm your identity with two or more pieces of evidence such as a password and a security code sent to your mobile phone. Using multi-factor authentication makes it more difficult for someone to gain access to your online accounts.

For more information about creating strong passwords and multi-factor authentication, visit the Stay Smart Online website.

Check your account statements

Monitor your account transactions online or using paper account statements if you receive them. If you spot any purchases you didn’t make, report these immediately to your financial institution.

Check your credit report

Request a copy of your credit report to check if it includes any unauthorised loans or applications.

Credit reporting bodies may hold different information about you, so you may need to request a copy of your credit report from all three credit reporting bodies.

If you suspect fraud, you can request a ban on your credit report. We recommend that you make the request to all three credit reporting bodies in case they maintain a consumer credit report on you.

Government-issued identity document information

If you have any questions about government-issued identity document information (such as your driver licence, Medicare card or passport), contact the agency that issued the identity document for advice.

Protect yourself from identity fraud.

Health information

If you have any questions about health information that a data breach notification doesn’t answer, contact your health service provider using the contact details on their website or in the phone book.

If you suffer distress, contact your doctor, a support service or your family or friends.

Sensitive information

If you have any questions about sensitive information that a data breach notification doesn’t answer, contact the organisation or agency that sent the data breach notification.

If you experience distress, contact your doctor, a support service or your family or friends. If your physical safety is at risk, contact the police.

If you experience online harassment, racism or abuse, visit the Office of the eSafety Commissioner website for information on keeping safe online.

Tax file number and tax-related information

If you have any questions about your tax file number or other tax-related information that a data breach notification doesn’t answer, contact the Australian Taxation Office (ATO). The ATO can monitor any unusual or suspicious activity with your tax file number.

Protect yourself from identity fraud.

Related

What is a notifiable data breach?
A data breach that may cause serious harm must be reported

Identity fraud
What to do if your identity has been stolen

Next Page

Acknowledgement of Country
We acknowledge the traditional custodians of Australia and their continuing connection to land, sea and community. We pay our respects to the people, the cultures and the elders past, present and emerging.

TWA Week 1 Practical Exercises

my student ID

document structure for exercise6.html

Exercise 4 Exercise 5 Exercise 7

Notifiable Data Breaches Scheme

What is a notifiable data breach?

Under the Notifiable Data Breaches scheme, an organisation or agency that must comply with Australian privacy law has to tell you if a data breach is likely to cause you serious harm.

Examples of serious harm include:

- identity theft, which can affect your finances and credit report
- financial loss through fraud
- a likely risk of physical harm, such as by an abusive ex-partner
- serious psychological harm
- serious harm to an individual’s reputation

An organisation or agency must also tell us about a serious data breach.

Generally, an organisation or agency has 30 days to assess whether a data breach is likely to result in serious harm.

When a data breach occurs, we expect an organisation or agency to try to reduce the chance that an individual experiences harm. If they’re successful, and the data breach is not likely to result in serious harm, the organisation or agency doesn’t need to tell the individual about the data breach.

How you’ll be told of a data breach

An organisation or agency may tell you about a data breach in an email, text message or phone call. The notification should include:

- the organisation or agency’s name and contact details
- the kinds of personal information involved in the breach
- a description of the data breach
- recommendations for the steps you can take in response

If an organisation or agency isn’t able to contact everyone they need to, they must put the data breach notification on their website. They must also promote this data breach notification, for example, through social media, news articles or advertisements.

Find out what to do when you get a data breach notification.

If you think you’ve not been told about a data breach

If you think that a data breach may affect your personal information and you’ve not been told, contact the organisation or agency that experienced the breach and ask them for information about the data breach (including whether your personal information was affected).

If they don’t respond to your complaint, or you’re not satisfied with their response, you may complain to us.

How to spot a phishing scam

A phishing scam is an attempt by scammers to trick you into giving them your personal information, such as your bank account details or passwords.

Avoid clicking on links in emails, or sharing your personal information on the phone or by email, unless you’re certain the organisation or agency that has contacted you is genuine. Contact the organisation or agency instead through publicly available contact details (such as the phone book or their website).

For more information about protecting yourself against scams, visit Scamwatch

Related

Notifiable Data Breaches Report July to December 2020
Statistical information about notifications received under the Notifiable Data Breaches (NDB) scheme

Responding to a data breach notification
Take action quickly to reduce your risk of harassment

Tips to protect your My Health record
How to safeguard your health Information

Identity fraud
What to do if your identity has been stolen

Next Page

Acknowledgement of Country
We acknowledge the traditional custodians of Australia and their continuing connection to land, sea and community. We pay our respects to the people, the cultures and the elders past, present and emerging.

TWA Week 1 Practical Exercises

my student ID

document structure for exercise7.html

Exercise 4 Exercise 5 Exercise 6

Notifiable Data Breaches Scheme

Notifiable Data Breaches Report: July-December 2020

About this report

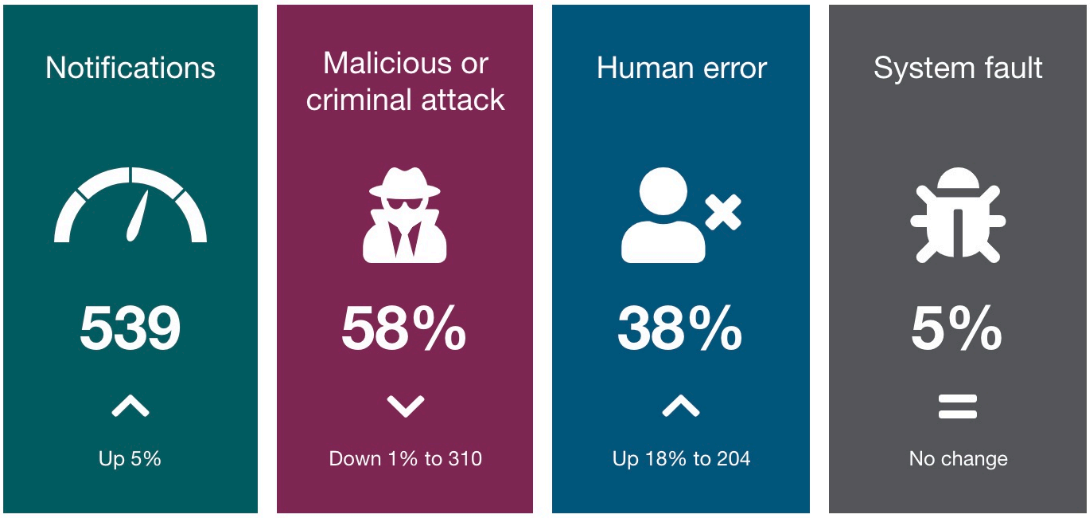
The Office of the Australian Information Commissioner (OAIC) periodically publishes statistical information about notifications received under the Notifiable Data Breaches (NDB) scheme to assist entities and the public to understand the operation of the scheme. This report captures notifications made under the NDB scheme for the period from 1 July to 31 December 2020.

NDB scheme statistics in this report are current as of 8 January 2021. However, a number of notifications included in these statistics are still under assessment and their status and categorisation are subject to change.

Executive summary

The NDB scheme was established in February 2018 to improve consumer protection and drive better security standards for protecting personal information. Under the scheme, any organisation or government agency covered by the Privacy Act 1988 must notify individuals affected and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

The OAIC publishes twice-yearly reports on notifications received under the NDB scheme to track the leading sources of data breaches, and to highlight emerging issues and areas for ongoing attention by regulated entities.



Comparisons are to the period from 1 January to 30 June 2020. These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category.

Key findings for the July to December 2020 reporting period:

1. 539 breaches were notified under the scheme, an increase of 5% from the 512 notifications received from January to June 2020.
2. Malicious or criminal attacks (including cyber incidents) remain the leading source of data breaches, accounting for 58% of notifications.
3. Data breaches resulting from human error accounted for 38% of notifications, up 18% from 173 notifications to 204.
4. The health sector remains the highest reporting industry sector, notifying 23% of all breaches, followed by finance, which notified 15% of all breaches.
5. The Australian Government entered the top 5 industry sectors to notify data breaches for the first time, notifying 6% of all breaches.
6. 68% of data breaches affected 100 individuals or fewer.
7. 78% of entities notified the OAIC within 30 days of becoming aware of an incident that was subsequently assessed to be an eligible data breach.

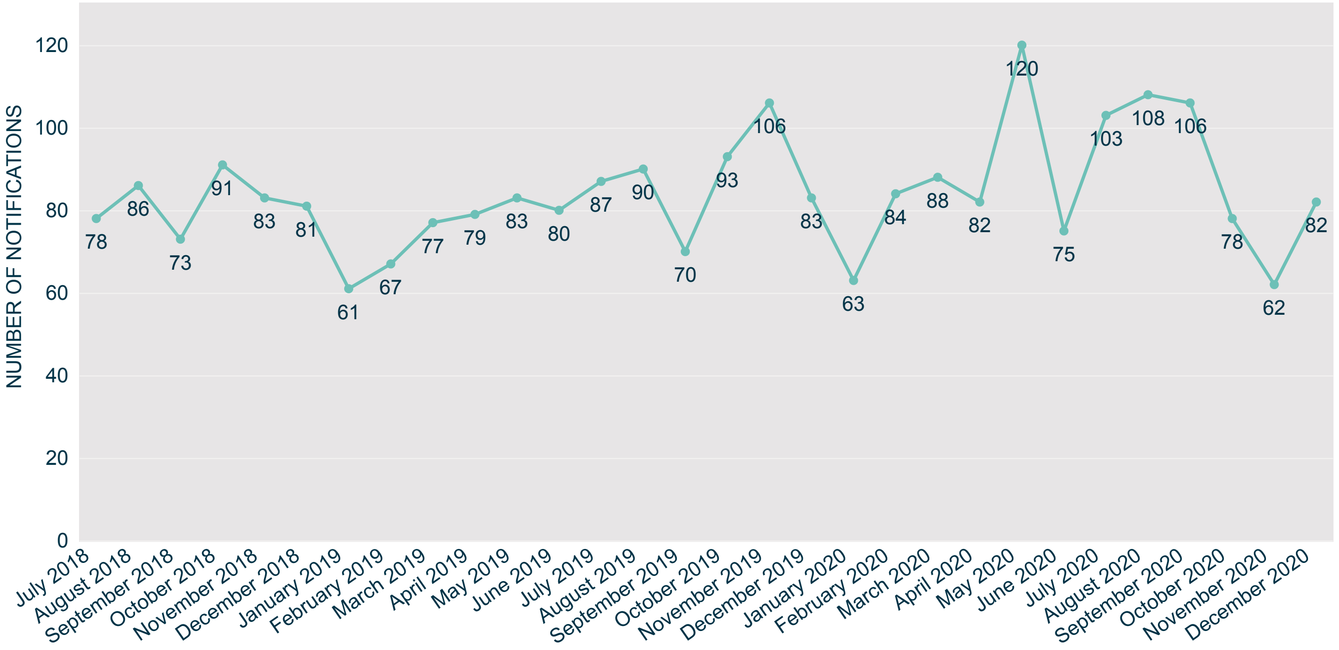


Chart 1 - Data breach notifications under the NDB scheme

Notifications received July to December 2020

The OAIC received 539 notifications this reporting period. This is a 5% increase compared to the previous 6 months and a 2% increase compared to the same period in 2019.

There was significant variation in the number of notifications received each month of the reporting period. The OAIC received 62 notifications in November - the second lowest monthly total since the NDB scheme commenced in February 2018 - but more than 100 notifications in July, August and September.

This reporting period saw continuation of the trend towards a greater proportion of data breaches attributed to human error. Data breaches resulting from human error accounted for 38% of all notifications, compared to 34% the previous 6 months and 32% in the same period in 2019.

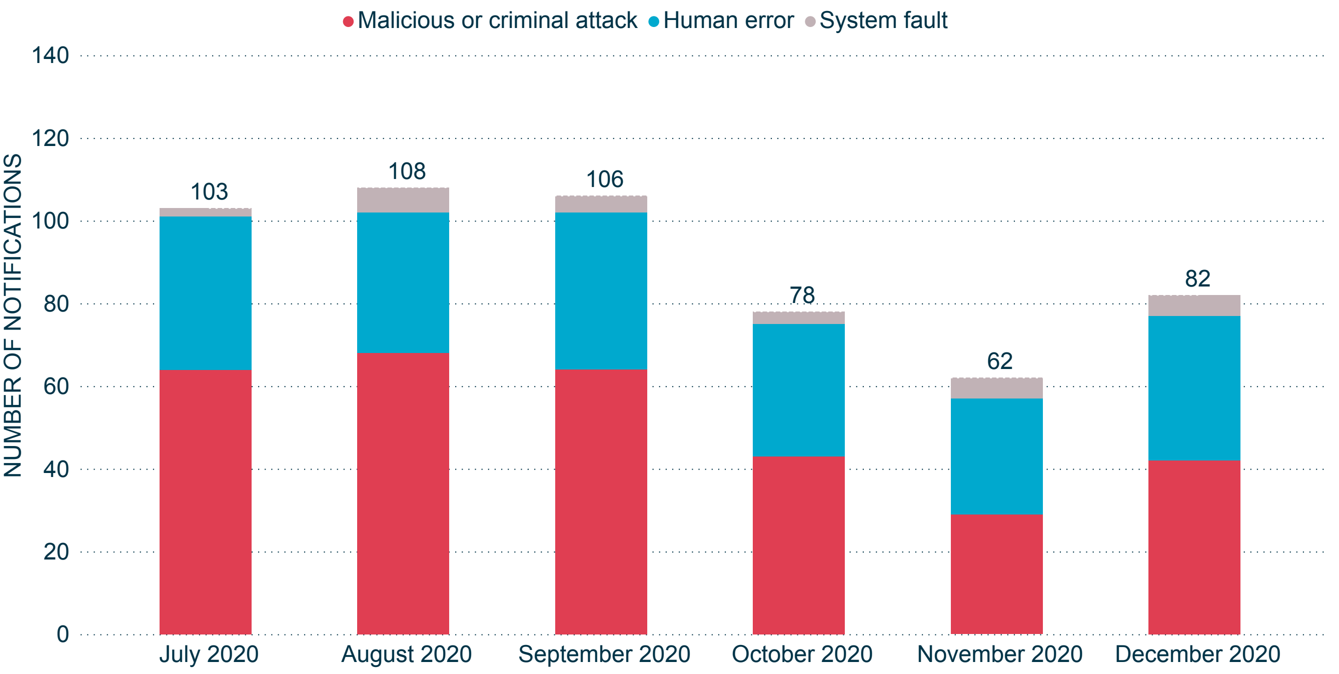


Chart 2 - Number of breaches reported under the NDB scheme - All sectors - showing attributed reason for breach

The impact of remote working arrangements resulting from COVID-19 restrictions

In early 2020, businesses across Australia introduced remote working arrangements in response to the COVID-19 pandemic. The OAIC has highlighted the privacy risks arising from these arrangements, recommending that entities consider undertaking privacy impact assessments to screen for unexpected privacy issues and to help mitigate any privacy risks associated with remote working arrangements.

Across the reporting period, the OAIC has closely monitored trends in NDB scheme notifications for any indications that remote working arrangements have either increased the risk of data breaches or impacted the capacity of notifying entities to meet their obligations under the Privacy Act.

Considering the public reporting on the increase in both COVID-19-themed fraud and the vulnerability of entities with remote working arrangements to cyber security incidents, it is noteworthy that there has only been a modest increase of 5% in the total number of notifications compared to the previous reporting period.

However, it is also notable that data breaches resulting from human error have significantly increased, both in terms of the total number received - up 18% - and proportionally - up from 34% to 38% of all notifications. While it is possible that this increase is linked to changed business and information handling practices resulting from remote working arrangements, the OAIC is yet to identify any information or incidents that conclusively prove a link.

Data breaches attributed to malicious or criminal attacks, including cyber incidents, have decreased both in terms of the total number received and proportionally, albeit only slightly. Breaches attributed to cyber security incidents decreased from 218 last reporting period to 212. This represents a decrease of 3%, roughly in line with the previous 6-monthly comparison.

This downward trend, particularly in relation to data breaches arising from cyber incidents, followed the Australian Cyber Security Centre’s 2019-20 Annual Cyber Threat Report highlighting an increase in reported spear phishing campaigns and COVID-19-themed malicious cyber activity during the pandemic. However, not all cyber security incidents reported to the Australian Cyber Security Centre constitute eligible data breaches under the NDB scheme.

The OAIC considers that more data and analysis are required before a view can be developed on the impact of remote working arrangements on the capacity of entities to securely manage personal information.

First Page

Acknowledgement of Country
We acknowledge the traditional custodians of Australia and their continuing connection to land, sea and community. We pay our respects to the people, the cultures and the elders past, present and emerging.