Community College Northern Inland

RTO 90027

Notification of Data Breach

A security incident recently experienced by Community College Northern Inland (**CCNI**) may have resulted in unauthorised access to personal information CCNI holds about some of its current and former students. We are issuing this notice to inform and protect our students.

This notice only affects you if you sent an email containing personal information (for example, an enrolment form) to inverell@communitycollegeni.nsw.edu.au or invadmin@communitycollegeni.nsw.edu.au between 2016 and July 2022. The security incident did not affect any other email address.

What happened?

On 24 May 2022, CCNI became aware that a series of phishing emails had been sent from email account inverell@communitycollegeni.nsw.edu.au. A further series of phishing emails were sent from email account invadmin@communitycollegeni.nsw.edu.au on 22 July 2022. Upon becoming aware of the incidents, CCNI sought assistance from its IT service provider to reset all passwords on the accounts and launched an investigation.

Our investigation discovered that an unknown person obtained unauthorised access to the inverell@communitycollegeni.nsw.edu.au and invadmin@communitycollegeni.nsw.edu.au email accounts (the "**compromised accounts**") between 19 May and 12 August 2022.

The compromised accounts contained various types of personal information in emails and attachments. There is no evidence that the intruder accessed any of the personal information contained in the compromised accounts. However, as that is a possibility, we are publishing this notice to inform individuals of the incident and suggest measures they may take to reduce their risk of harm.

Along with a thorough forensic investigation of the incident, we have also implemented several technical and practical measures to improve the security of our email accounts in order to ensure that this kind of incident does not reoccur in future.

We have reported the incident to the Office of the Australian Information Commissioner. We will continue to liaise with that authority regarding the incident and we will ensure that all of our statutory responsibilities are met.

What personal information was affected?

The compromised accounts included copies of enrolment forms for some students, which contained personal information including:

- contact information (such as name, address, email address and phone number);
- gender and date of birth;
- country of birth, citizenship, Aboriginal or Torres Strait Islander status;
- languages spoken, education history, employment status and living situation; and
- disability information.

Enrolment forms may have also been accompanied by scanned copies of driver's licences or other identification documents.

The compromised accounts may have also included payment forms including credit card or bank account details.

The above information does not relate to all CCNI students; we currently believe that the compromised accounts only contained the personal information of a few hundred current and former students at most. We are currently conducting automated and manual searches to identify the specific personal information which was contained in the compromised accounts. Once these searches are complete, we will contact each of the specific individuals whose personal information is affected.

Steps you can take to protect against potential misuse of personal information

To date, there is no evidence that any of the above personal information has been published or misused. Nevertheless, as this is a possibility, we wanted to let our students know the steps they can take to protect themselves against any potential misuse of their personal information.

Identification documents

Driver's licences and other identification documents can be used to commit identity fraud. This means that a fraudster could use those details to attempt to impersonate you to obtain a benefit or service. For example, they could attempt to open a bank account, obtain a credit card, redirect your mail or port your mobile phone.

To minimise this risk, it is important to remain vigilant for signs of identity fraud. We recommend that:

- you should review your financial accounts for suspicious activity, such as unauthorised transactions and requests to change account details, and notify your financial institution as soon as possible if you notice any such activity;
- if you find you are not receiving mail, you should check with Australia Post that your mail has not been redirected, and secure your letterbox – fraudsters sometimes redirect or steal mail to avoid detection;
- if you notice that your mobile phone loses coverage for an extended period of time, you should check with your telecommunications provider that no-one has attempted to port your phone to another provider – fraudsters sometimes port mobile phones to gain access to SMS authentication messages; and
- if you receive goods or services that you did not order, or notifications about goods or services that you did not order, you should notify the relevant seller or service provider as soon as possible.

You should also periodically check your consumer credit report for unauthorised activity. You can apply for an annual free credit report from Australia's three credit reporting agencies: Equifax, Experian and illion. This report will also show you which organisations have recently checked your credit history, so you can tell them not to authorise a new account in your name. You can also request that a ban be put in place while you investigate further.

If you are concerned that your driver's licence details may have been misused, you should contact the relevant driver licensing agency in your State or Territory and explain that your driver's licence details have been involved in a data breach.

If you believe that you are the victim of identity fraud, you can report the matter to the police through ReportCyber.

Medicare numbers and Centrelink CRNs

Your Medicare number or Centrelink CRN could be used to impersonate you in an attempt to obtain government benefits. If you think your Medicare number or Centrelink CRN may have been affected, you can contact the Services Australia Scams and Identity Theft Helpdesk on 1800 941 126 or reportascam@servicesaustralia.gov.au and explain that your Medicare number or Centrelink CRN has been involved in a data breach. They will apply protective measures on your Medicare or Centrelink account to prevent anyone impersonating you to obtain benefits.

It is also possible that a fraudster may contact you pretending to be from Services Australia or another government agency or business in an attempt to scam you or trick you into disclosing other personal information or access credentials. To protect yourself against scams and social engineering:

- be careful of unsolicited emails, SMS messages or telephone calls which purport to be from CCNI or a government authority or business;
- be wary of anyone contacting you who requests personal information or access credentials from you, even if they appear to know some details about you;
- if you are in doubt about whether a telephone call is genuine, hang up and call the authority or business back on their public telephone number;
- for emails, check the sender's address is the authority's or business's real email address - fraudsters may send emails from look-alike addresses; and
- do not respond to email or SMS messages asking for personal information – few legitimate organisations will ask for personal information by email or SMS.

Credit card details

There is currently no evidence that any of the stolen data has been misused. Nevertheless, there is a small chance the intruder could use your credit card details to purchase goods and services.

If you think your credit card details may have been affected, we strongly recommend that you contact the issuing bank as soon as possible and inform them that your card details have been involved in a data breach.

They will provide you with advice and may issue you with a replacement card. You should also review your credit card statements carefully to identify any suspicious transactions.

Bank account details

Simply knowing your bank account number is not enough to allow an unauthorised person to access your bank account. However, it is possible that a fraudster may contact you pretending to be from your bank or another business or government agency in an attempt to scam you or trick you into providing more personal information or access credentials to your bank account. To protect yourself against scams and social engineering:

- be careful of unsolicited emails, SMS messages or telephone calls which purport to be from CCNI or a government authority or business;
- be wary of anyone contacting you who requests personal information or access credentials from you, even if they appear to know some details about you;
- if you are in doubt about whether a telephone call is genuine, hang up and call the authority or business back on their public telephone number;
- for emails, check the sender's address is the authority's or business's real email address - fraudsters may send emails from look-alike addresses; and
- do not respond to email or SMS messages asking for personal information – few legitimate organisations will ask for personal information by email or SMS.

Disability information

The enrolment form contained a question asking whether the student has particular categories of disability. It did not contain any further details. We appreciate that this type of information is sensitive in nature, and that the fact that such information may have been subject to unauthorised access may be distressing. We sincerely regret and apologise for any distress that this incident may have caused you. If you experience distress, you should consider consulting a support service or your GP.

Additional information

Additional guidance steps you can take to protect yourself following a data breach can be found at the Office of the Australian Information Commissioner's website.

You can also get advice and support by contacting IDCARE, Australia's national identity & cyber support service on 1800 595 160. IDCARE has fact sheets about identity fraud and scams on its website.

If you still have questions

CCNI takes the security of your personal information very seriously and we sincerely regret any inconvenience this incident may cause you.

If you would like to discuss the situation with us further or if you require further guidance on how to protect your personal information, please do not hesitate to contact us at help@ccni.nsw.edu.au and **0428 498 171**.