22 November 2022

Xavier College – Email Incident

Dear Old Xaverians

In June this year, Xavier College became aware that the email account of one of its employees had been subject to unauthorised access by an unknown third party.

The College immediately notified any members of our community directly affected by the unauthorised access.

In late October it came to our attention that an unauthorised third party may disclose details of these mailbox contents.

On each occasion, the College undertook the following steps in response:

Engaged cyber security experts to provide an in-depth investigation
- Took steps to ensure the incident was contained and that our network and data systems had not been adversely impacted and were secure
- Conducted a review of the individual's Mailbox contents to identify any individuals who may have been at-risk
- Notified any members of our community potentially affected by the data breach
- Consolidated ongoing training for staff and students around cyber vigilance and online safety

We also notified the Office of the Australian Information Commissioner and Australian Cyber Security Centre of the incident.

The College has now taken steps to re-assess the original data and consider whether any further individuals may have been affected.

As in June, immediate notification to specific individuals is occurring.

As you will be aware, there has been a proliferation of cyber attacks and data security issues (including a number of other schools) reported over recent months.

As a general reminder, we attach recommendations for steps you can take to protect your personal information (see "Steps you can take to protect against potential data misuse").

Please remain vigilant regarding your online security and ensure you do not open any suspicious emails or links.

If you have any questions or require support regarding this matter, please utilise our dedicated email at cyber@xavier.vic.edu.au

Kind regards

Xavier College

Steps You Can Take to Protect Against Potential Data Misuse

What can I do to protect my personal information?

- be aware of email, telephone and text-based scams and refrain from sharing your personal information until you are certain about who you are sharing it with;

- enable multi-factor authentication for your online accounts where possible;

- ensure you have up-to-date anti-virus software installed on any device you use to access your online accounts;

- take note of what is called a 'Uniform Resource Locator' or 'URL' when on a webpage which is asking for your login credentials. This is located in the address bar of your web browser and typically starts with 'https://'. If you are suspicious of the address, do not provide your login details and contact your service provider to ensure you are logging into the correct page;

- do not open suspicious texts, pop-up windows or click on links or attachments in emails – delete them;

- do not respond to phone calls about your computer asking for remote access; and

- choose passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper and lower-case letters, numbers and symbols. Do not use the same password for every account/profile, and don't share your passwords with anyone.

For further guidance around securing your personal information and protecting yourself from scams, we encourage you to utilise these resources:

- https://www.cyber.gov.au/acsc/view-all-content/publications/easy-steps-secure-your-online-information

- https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams/

- https://www.oaic.gov.au/privacy/your-privacy-rights/tips-to-protect-your-privacy/