## Steps can you take to protect your information online

### General guidance

The most common risk associated with any unauthorised access to personal information is phishing emails and scams. Scam calls and phishing emails are becoming increasingly sophisticated and can appear to come from legitimate phone numbers with local area codes. They will often claim to be calling from a reputable organisation, such as a government entity, bank, or telecommunications agency. They will also create a sense of urgency to try to get you to disclose sensitive information or to elicit funds from you.

Listed below are some precautionary steps you can take to help improve your online safety and protect your information from potential misuse:

- be aware of email, telephone and text-based scams. Do not share personal information with anyone unless confident about who you are sharing it with;
- remain alert for any phishing scams that may come to you by phone, post or email;
- when on a webpage asking for your login credentials, take note of the web address or URL ('Uniform Resource Locator'). The URL is located in the address bar of your web browser and typically starts with https://;
- if you are suspicious of the URL, do not provide your login details. Contact the entity through the usual channels to ensure you are logging into the correct web page;
- enable multi-factor authentication for your online accounts where possible, including your email, banking, and social media accounts;
- ensure you have up-to-date anti-virus software installed on any device you use to access your online accounts;
- review your recent transaction history and bank statements for any suspicious activity. Contact your bank in the instances where suspicious activity is identified;
- confirm the security of your online accounts by checking the strength of your passwords and whether they have been involved in any data breaches on the NSW Government password checker website: https://www.nsw.gov.au/id-support-nsw/passwords;
- follow the Australian Competition and Consumer Commission's Scamwatch guidance for protecting yourself from scams here: https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams/; and
- for more information, visit the OAIC's tips for further guidance about protecting your identity:
    - https://www.oaic.gov.au/privacy/your-privacy-rights/tips-to-protect-your-privacy/ and
    - https://www.oaic.gov.au/privacy/data-breaches/data-breach-support-and-resources/.

### Who can I contact for more information about cyber security incident?

We are committed to supporting affected individuals and our wider College community. If you have any questions, we encourage you to contact us at dataenquiry@bne.catholic.edu.au.