21 June 2019

Dear Parents and Carers,

Catholic Education Western Australia (CEWA) has been advised of recent incidents where employees in the organisation may have been targeted in an attempted cyber-attack.

CEWA has systems and measures in place to monitor and respond to cyber security incidents and continues to work closely with cyber security experts to mitigate and address a potential breach. In instances where a breach may have occurred, CEWA follows a stringent reporting process including notification to those who may be affected.

Potential incidents of this nature are a timely reminder that cyber security is something that all members of our school community should be aware of.

As cyber security incidents become more sophisticated, it is important to be aware that they may take the form of emails from people you don't know, may appear to be from a person you may know, or may actually be sent via individual accounts.

It is important to be vigilant and take notice of the language used, the type of email (blank email body, or including links or attachments), and what the domain or the link actually points to.

To best protect the security of your personal information, it is suggested that online passwords are regularly changed, that you carefully review the sender of emails and be cautious of links and attachments. You may also want to consider checking that the anti-virus software installed on your electronic devices is up to date.

If you believe you have been impacted, or have clicked on a link: Install an Anti-Virus tool and scan all home computers.

- (https://www.malwarebytes.com/ or https://home.sophos.com/ provide free Anti-Virus software)
- Review your email account for misuse and signs of intrusions – unusual forwarded emails, mail rules, new sent items

Check for signs your account has been hacked

- Your password may have been changed
- Unusual inbox activity – for example, if you stop receiving email to your inbox, but can send emails without a problem
- You are receiving unexpected emails that appear different to your usual junk mail
- People you know advise you about unusual emails and random links
- Your system is acting up - redirected internet searches, unexpected installs, rogue mouse pointers

If you discover you have been impacted:

- Make sure you can still login and change your password immediately
- If the same password is being used to log into other applications, change your passwords immediately
- If required, contact your service provider (email/internet)
- Check and register email addresses and/or credentials at https://haveibeenpwned.com/
- Check sent items to see what emails have gone out and notify people if you are concerned that spam emails may have been sent to them from your account

Yours sincerely

Ian Hagen

Principal