HOW TO PROTECT YOUR FAMILY'S ONLINE PRIVACY

Most people cannot imagine a day without using some form of a digital device. While digital devices have many benefits, technology can potentially compromise your personal information and that of your family. It might surprise, if not shock you, to realise how easy it is for people to discover anything and everything about you. From your household income and personal address, to your children's names and what toppings they like on their pizza.

Thankfully, this is something you can rectify by improving your online habits and changing a few privacy settings. With the end of the year approaching fast, why don't you make this a New Year's resolution and enjoy better protection for you and your family.

Here are a few simple ways in which you can do this:

01 Clean up your digital security hygiene game

When opening an account, make sure you use strong passwords that cannot easily be traced back to you. Change them regularly for safety purposes. Do not use the same password for all your different accounts; if it gets compromised once, criminals will be able to access all your details easily from there. If you're worried about forgetting a variety of passwords, there are various options available that can provide strong passwords and store them safely in online vaults. LastPass is a free option that can be downloaded on desktop and smart devices that run Android or iOS. 1Password charges a small fee for their service and allows you to save passwords on their app safely.

Furthermore, you should have two-factor authentication in place with your important accounts. This is when you need to provide your mobile number to receive a text with an additional number in order to log into your account. Lastly, make sure your devices are up to date with the latest security updates available for your software.

02 Don't blindly trust every message you receive

If you get a message from your bank suddenly demanding a username and password by telling you that you have been hacked or your account has been compromised, don't just comply. This is a common strategy used by criminals trying to scare or trick you into giving them access to your accounts. Don't react straightaway, as tempting as it is. Think carefully and start checking. You might pick up that something is fishy in the grammar or spelling, as well as strange links in the message that have nothing to do with the bank or organisation they are supposed to be representing. However, the truth of it is, criminals are getting smarter and they can copy banking communications pretty well. Do not call the number on the email. The best thing to do, is to call your bank independently, on a number you have for them or that you have looked up independently. Ask your bank to check your account and explain the mail you have received.

The same goes for emails from people you do not know. Never open an attachment from someone you do not know, or an email that appears out of character, no matter how enticing it may look. Attachments on criminally motivated e-mails contain code which is used to gain access to your personal data.

03 Delete any apps you're not actively using

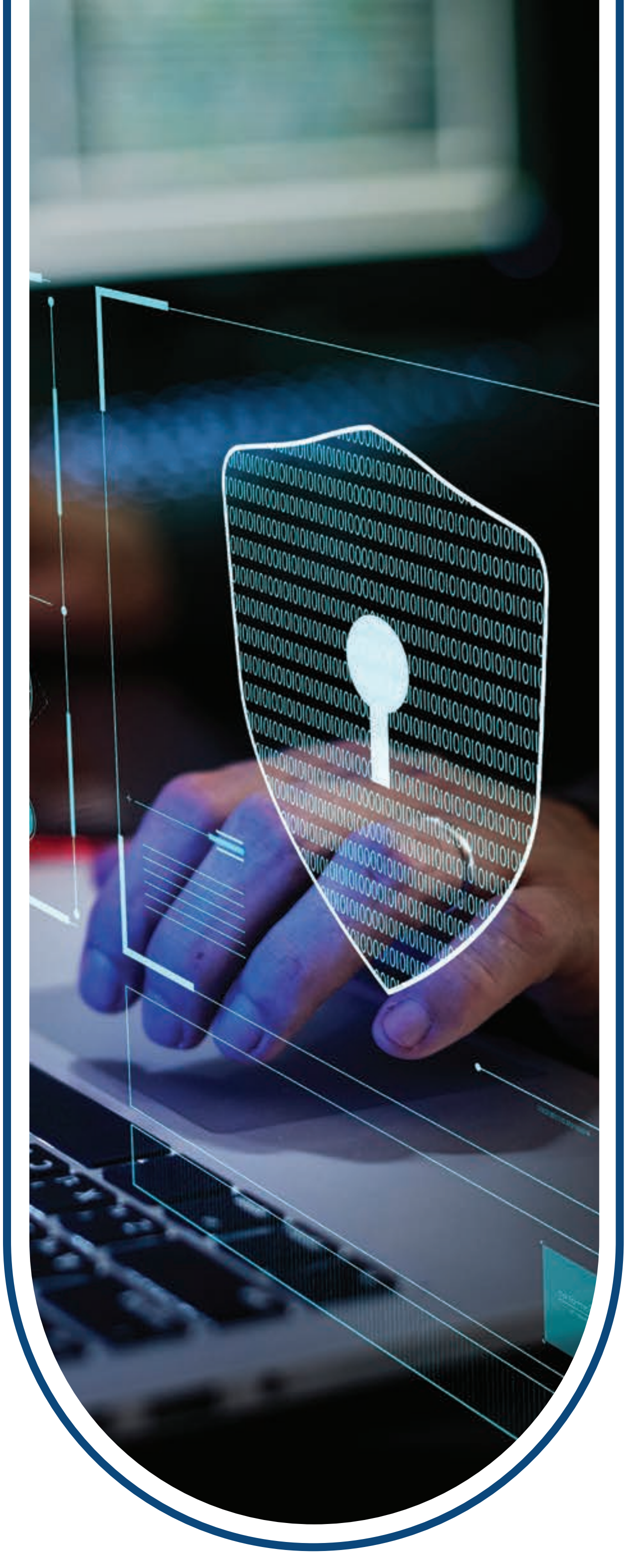
Remember, your information is valuable, and app developer companies can sell any information they gather from your devices for profit. So be careful what you download. Always read the terms and conditions so you understand fully what you are providing access to when you download a new app. Also, it's often better to use browsers to complete certain tasks than download new apps. This way, there's less information about you that's accessible to the developers.

04 Turn off your ad personalisation wherever possible

It's worth the time to go into your settings regularly to update your settings and disallow ad personalisation, because this gives companies the opportunity to conduct invasive tracking of your movements and preferences.

05 Social media permissions

When you join any social media platform like Facebook, Instagram or Twitter, you will be able to predetermine certain levels of privacy in the settings. It's important to read the terms and conditions during setup. If you have been using any of these platforms for some time, you can still go into your profile and re-set your privacy settings. Take the time and ensure you have the optimal protection.



Bottom line

Protecting your online presence might feel like a daunting task. However, just by taking some small steps to practice better digital habits can make a big difference. As time goes on it helps to read up and do your research. Information changes and hackers, phishing experts and scammers will keep coming up with new ways to access your information.

Always take heed of warnings sent to you by your bank or employers. This way, you can move into 2021 with better passwords, improved security and more peace of mind!

If you or your loved one needs support during this time, reach out to your ICAS EHWP via your toll-free number to seek counselling support. Alternatively, download the ICAS On-the-Go App and login with your Company App Code.

Call your dedicated **Toll-Free Line.**

(Free from landline and mobile phones.)

Or request a call back: ***134*905#**

Applicable to you and those who live under your roof.

References:
https://www.forbes.com/sites/theyec/2019/11/12/nine-important-tips-to-protect-your-online-privacy-and-security/?sh=2121fb123c16
https://thenextweb.com/basics/2019/08/25/dont-be-an-idiot-heres-how-to-store-and-remember-all-your-passwords/