



26 October 2020

Media release

Six steps for digital self-defence during Australian Cyber Week 26-30 October 2020

The Australian Digital Health Agency is promoting six practical steps for digital self-defence against attacks such as phishing and ransomware. These steps can protect your work and personal information.



1. *Build security awareness with the [Digital Health Security Awareness eLearning course](#)*
2. *Keep your software up to date*
3. *Use strong [passwords](#) and implement [multi-factor authentication](#)*
4. *Back up your data regularly*
5. *Do not respond to unsolicited [phishing](#) emails, texts and calls*
6. *If you fall victim to [ransomware](#), avoid paying the ransom*

Tony Kitzelmann, the Agency's Chief Information Security Officer said "Like a scheduled health check-up, we encourage everyone to take time during **Australian Cyber Week** to review their online presence, to ensure the appropriateness of their published personal and professional information and check if it puts them at risk from a targeted cyber-attack."

2020 has been a year where many people and organisations have relied on virtual interactions to keep in contact and to conduct business. While there are many benefits to this increased connectivity, cyber-criminals will take every opportunity to exploit any vulnerabilities to steal your data or funds.

The latest Australian Cyber Security Centre threat report¹ identifies that threats 'against Australia's national and economic interests are increasing in frequency, scale, and sophistication.'

The economic cost of cyber-crime to Australia, is difficult to quantify however, industry estimates have previously placed cyber security incidents as high as \$29 billion annually.²

The healthcare sector stands out as a tempting target because of the critical nature of healthcare services and the high value placed on health data in the black market. So, now is a good time to learn how to defend yourself and your organisation against these threats.

For the more than 22 million Australians with a My Health Record there are multi-tiered [security controls](#) to defend the system from malicious attack. The system has been built and tested to Australian Government standards to protect the confidentiality, integrity, and availability of information within an individual's My Health Record.

¹ ACSC Annual Cyber Threat Report, July 2019 to June 2020. <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020>

² Frost & Sullivan study commissioned by Microsoft 2018 <https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costsaustrian-businesses-29-billion-per-annum/>



For more information about Cyber Security visit:

Australian Digital Health Agency

[Cyber Security Centre](#)
[Digital Health Security Awareness Course](#)
[Cyber Security Podcasts](#)

Australian Cyber Security Centre

[Cyber Security for individuals & families](#)
[Cyber Security for small & medium businesses](#)
[Cyber Security for large organisations & infrastructure](#)

Australian Cyber Week

26-30 October [Schedule of events](#)

Media contact

Media Team

Mobile: 0428 772 421 Email: media@digitalhealth.gov.au

About the Australian Digital Health Agency

The Agency is tasked with improving health outcomes for all Australians through the delivery of digital healthcare systems, and implementing [Australia's National Digital Health Strategy – Safe, Seamless, and Secure: evolving health and care to meet the needs of modern Australia](#) in collaboration with partners across the community. The Agency is the System Operator of [My Health Record](#), and provides leadership, coordination, and delivery of a collaborative and innovative approach to utilising technology to support and enhance a clinically safe and connected national health system. These improvements will give individuals more control of their health and their health information, and support healthcare providers to deliver informed healthcare through access to current clinical and treatment information. Further information: www.digitalhealth.gov.au.

The Digital Health Cyber Security Centre has been established to strengthen the security of our national digital health systems and services; and to promote increased security awareness and maturity across the digital health sector.