Australian Government

Australian Digital Health Agency

Think before you click

– protect your healthcare consumers

This document provides general security awareness information
and is not intended to be comprehensive.

Summary

Digital technology has become such an integral part of our daily lives, both at work and at home. As a society, we have become accustomed to browsing the internet, sending emails and using social media. So much so, that we don't always stop to consider the potential risks associated with use of this technology.

There's no question that the benefits of digital technology are huge, particularly for the health sector. As stated in Australia's National Digital Health strategy, *"Digital information can transform the quality and sustainability of health and care. Used effectively, it can help save lives, improve health and wellbeing and support a sustainable health system that delivers safe, high quality and effective health services for all Australians."*

However, to realise these benefits, we need to be vigilant to make sure we don't fall victim to a security incident, such as a malicious software attack or an online scam.

Given that **91% of cyberattacks** and the resulting data breach **begin with a spear phishing email**, it is important that we stop and consider the consequences before clicking on a link or attachment. To protect healthcare information, it's also essential that we stop and think before we send emails, publish social media posts and use wireless networks.

Emails

While email provides a fast, convenient way to send and receive information it's not always the best option, particularly for sensitive information. Email is also frequently used for scams, phishing and distribution of malicious software, so it is important to be on your guard when using email.

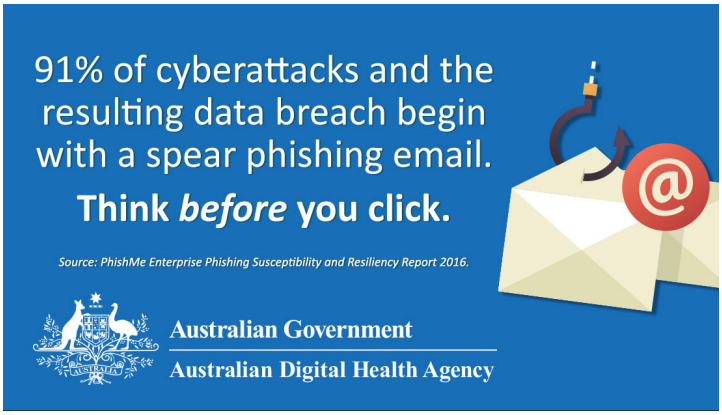
Before you click 'send', think:

Is this email appropriate, or would it cause damage to myself, my healthcare consumers or my employer if it fell into the wrong hands (or was made public)?

By default, email is not secure. Unless it is encrypted, email can be read during transmission, and consequently, unencrypted email should not be used to send sensitive information, such as healthcare information.

Before you click on the link in an email, think:

Is this a genuine email, or could it be a scam?



If you are unsure of whether an email is legitimate, do not click on links, open attachments or reply.

Additional information about phishing and using email safely is available on the Stay Smart Online website:

- Tips for using email safely:
  https://www.staysmartonline.gov.au/protect-yourself/protect-your-stuff/email
- Information about phishing:
  https://www.staysmartonline.gov.au/protect-yourself/recover-when-things-go-wrong/phishing

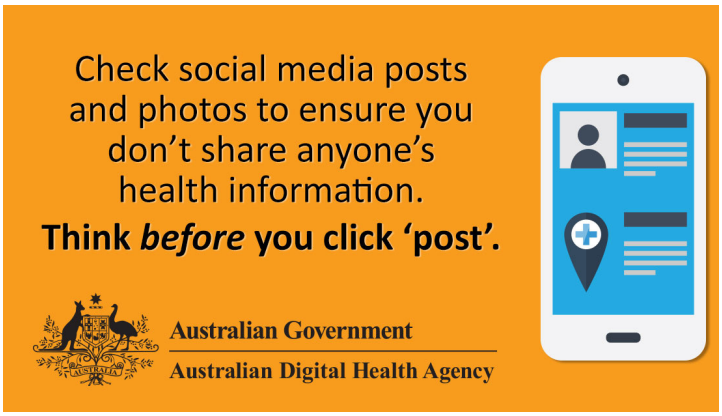
Further information about the latest scams is available on the ScamWatch website:

- 'The little black book of scams':
  https://www.accc.gov.au/publications/the-little-black-book-of-scams
- 'If it sounds too good to be true ... it probably is'
  - A leaflet containing tips on how to protect yourself from internet scams and spam:
  https://www.accc.gov.au/publications/if-it-sounds-too-good-to-be-true

Social media

Before you click 'post', think:

Should I be posting this information on a social media site, or would it cause embarrassment to me, my healthcare consumers or my workplace if it were known publicly?



Always take care to check images before posting – ensure there is nothing sensitive in the background of the image, such as healthcare consumers or their healthcare information (e.g. electronic records, paper files or information on a whiteboard).

It is also important to ensure that the maximum privacy settings are used on all social media platforms (but remember – this does not provide a guarantee, it just helps to reduce the risk of your information being accessed or compromised).

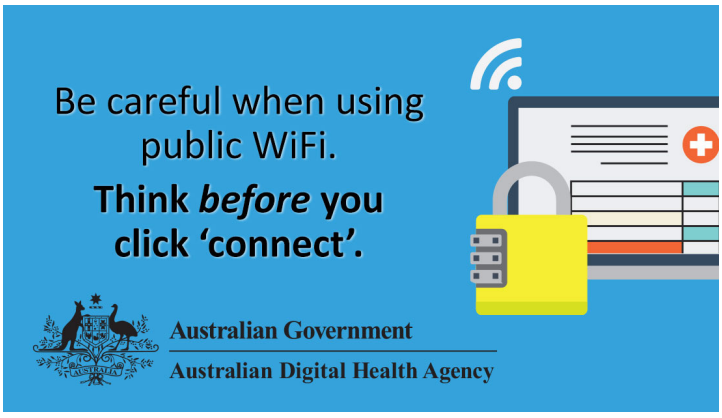
Remember:
Once you post something online, you have lost control of who accesses it and what they do with it.

More information about socialising online safely is available on the Stay Smart Online website:
https://www.staysmartonline.gov.au/protect-yourself/doing-things-safely/socialising-online

Wifi connections

Before you click 'connect', think:

Is this WiFi network secure?



Remember:
If you don't need to enter a password to connect to the WiFi, your connection isn't secure. With the right tools, anyone connected to the network can see the unencrypted information you send, and can also capture session cookies which can potentially allow the attacker to login as you, even if they don't know your username and password.

To improve security, you can install a reputable virtual private network (VPN) solution on your device to create an encrypted 'tunnel' that allows data traffic to pass securely over public Wi-Fi networks. Otherwise, it is best to limit use of public WiFi for general internet browsing and avoid entering sensitive information.

Additional information about using WiFi safely is available on the Stay Smart Online website:
https://www.staysmartonline.gov.au/protect-yourself/doing-things-safely/using-public-wireless-or-wifi-networks

Use our resources to share this message

The Australian Digital Health Agency has developed a range of social media tiles and posts that you can share across your social channels to help promote the message to 'Think before you click':

- Think before you click 'send' - Download image (JPG, 86.3KB)
- Think before you click links in emails - Download image (JPG, 125KB)
- Think before you click 'post' - Download image (JPG, 126KB)
- Think before you click 'connect' - Download image (JPG, 94.4KB)
- Suggested social media posts (PDF or Word versions available)

You can also access these resources, by visiting the Australian Digital Health Agency Website (www.digitalhealth.gov.au) and searching for 'Think before you click'.

Further information

Other useful sources of information include:

- Information Security Guide for Small Healthcare Businesses – guidance for non-technical health professionals on the topics of privacy, passwords, software updates, back-ups and staff security awareness (available on the Australian Digital Health Agency Website: www.digitalhealth.gov.au).
- Stay Smart Online (staysmartonline.gov.au) – a wide range of resources for individuals and small businesses, including a free alert service, which provides information about the latest online threats and how they can be managed.
- Scamwatch (scamwatch.gov.au) – information for individuals and small businesses about how to recognise, avoid and report scams, including Scamwatch Radar a free alerts service about the latest online scams.

Publication date: December 2017

Contact for enquiries

Telephone: 1300 901 001 or **email:** help@digitalhealth.gov.au

Disclaimer

The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Australian Government

Australian Digital Health Agency

www.digitalhealth.gov.au