

Cyber Safety Fact Sheet

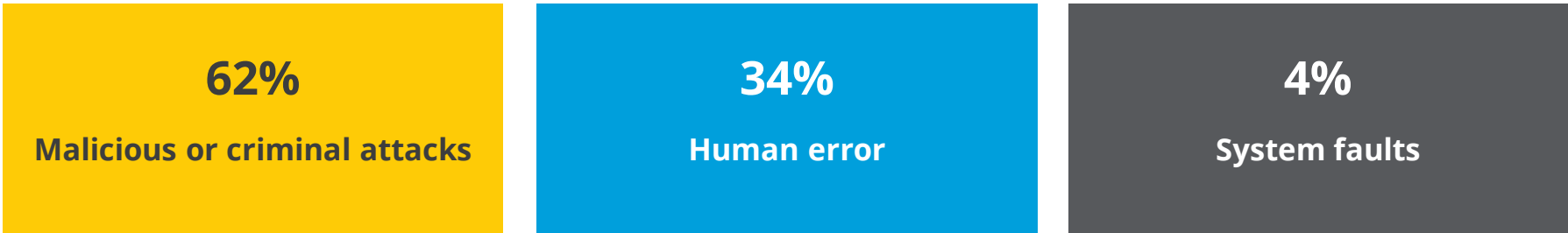
Cyber safety is everyone's responsibility!

At Northern Health, our goal is to protect our valuable information from unauthorised access. This is vital to uphold our patients trust in Northern Health as a reliable health care organisation.



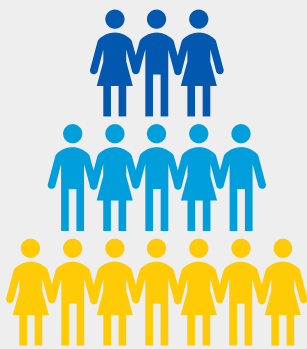
Did you know?

The majority of data breaches reported between 1 April 2019 and 30 June 2019 were due to malicious or criminal attacks, according to the Office of the Australian Information Commissioner (OAIC).



You are our best protection!

As employees of Northern Health, there are simple things we can all do to avoid a cyber security incident. The following guidelines sum up how we can be smart about what we do when we're online, whether we're at home or work.



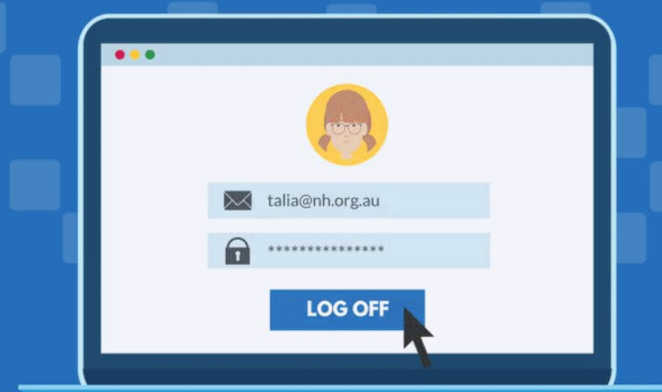
1. Keep all private information secure

- | | | | |
|---|--|---|--|
| Always keep all confidential and sensitive information secure and only use this information for the purpose it was collected. | Do not access information or data that you are <u>not</u> permitted to access. | Do not store patient information on external (non-Northern Health) systems or sites including personal storage devices. | Personal storage devices include USB devices, mobile phones and external cloud based storage sites like Dropbox and Office365. |
|---|--|---|--|

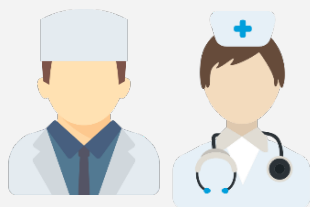
2. Always keep your usernames and passwords private

Your username and password act as your credentials. They authenticate your Northern Health identity, keep your personal information safe and give you access to your email.

You are responsible for any activity conducted with your username. If someone else is logged in with your account, you are responsible for any activities that occur.



Your username and password give you access to systems and information based on your role.



Doctors have full access to clinical record systems where they can create and change patient records.



Certain Payroll team members have access to payroll information where they can view and change staff banking details.

3. Safeguard your usernames and passwords

1

Create strong passwords and never share your username and password with anyone under any circumstance.

2

Never write your passwords down, save them in your browser, or store them unprotected in your computer.

3

Avoid using your Northern Health password for external (non-Northern Health) systems such as Facebook or LinkedIn.



Keeping your Northern Health password different from any other passwords you use ensures your Northern Health information remains protected even if your other passwords are stolen.



4. Use **passphrases** instead of passwords because they are more secure than a single word

A passphrase is a short phrase that is easy for you to remember. To create a passphrase, simply choose a phrase at least 13 characters long - it will not expire. Below are examples of passphrases.

Passphrase:
canariesarepurple

Passphrase:
tencentstothedollar

Passphrase:
likewaterforchocolate

Note: Please do not use these examples as your passphrase.

5. Lock your computer or device when you step away from it


Always log off your computer, laptop, or tablet when you are not using it.

If you leave your computer or device unattended while you are logged on, other people can see your personal information, or our patient’s records. They can also access all Northern Health systems and information that you have permission to access.




6. Keep your mobile devices secure


Mobile devices like tablets, phones and laptops present specific cyber safety issues. Make sure you always apply these best practices.




Use a pin code on your mobile or tablet.



Do not leave your laptop in full view in a car.



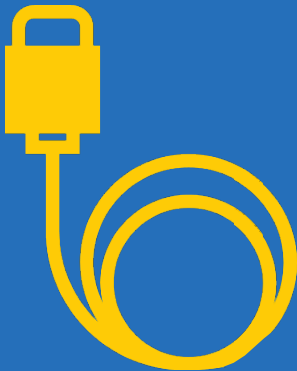
Keep software on your mobile devices up to date.



Avoid connecting to free WiFi hotspots because they are unprotected.

If you use a mobile device to access Northern Health information, this must be in accordance with the Northern Health [Knowledge and Information Management Policy](#).

7. Apply special care when using portable storage devices on the Northern Health network



Using portable storage devices on the Northern Health network can lead to the spread of malware which can damage Northern Health programs and systems.

Portable or removable storage devices can be small USB keys and memory cards, or larger removable hard drives which are sometimes used to back up systems. Because of their portability, these devices are often used extensively on the network to transfer data and/or information.

Problems can arise when portable storage devices are used on other networks, like other hospital networks or home networks. This increases the chances of the device picking up a virus especially if the other networks don't have adequate security.

Best practices for using a portable storage device

Only use a portable storage device if there is no other alternative.

Do not use a portable storage device that has been used on another network or at home.

Limit the use of portable storage to one device.

Do not discard a portable storage device supplied by Northern Health unless it's absolutely necessary.

Do not use a portable storage device if you do not know where it has been used.

Where possible, encrypt the device especially if it will be used to transfer information off the Northern Health network.



It's also easy to lose a portable storage device which exposes Northern Health to data loss issues.

8. Be aware of possible phishing attempts

Phishing, spear phishing and whaling are scams that try to trick us into giving away private information using messages, links or attachments that appear authentic, but they're not. Phishing emails may:

- ✓ Claim to be from a popular banking corporation or taxation office
- ✓ Attempt to verify your personal details due to a technical error which deleted customer data
- ✓ Include threatening actions if bills or fines are not paid immediately
- ✓ Warn you about unauthorised or suspicious activity on your account, or storage allowance issues
- ✓ Have a sense of urgency that requires immediate attention.

Characteristics of a phishing email

Incorrect grammar or spelling

Plain text or no logos

Requests personal information

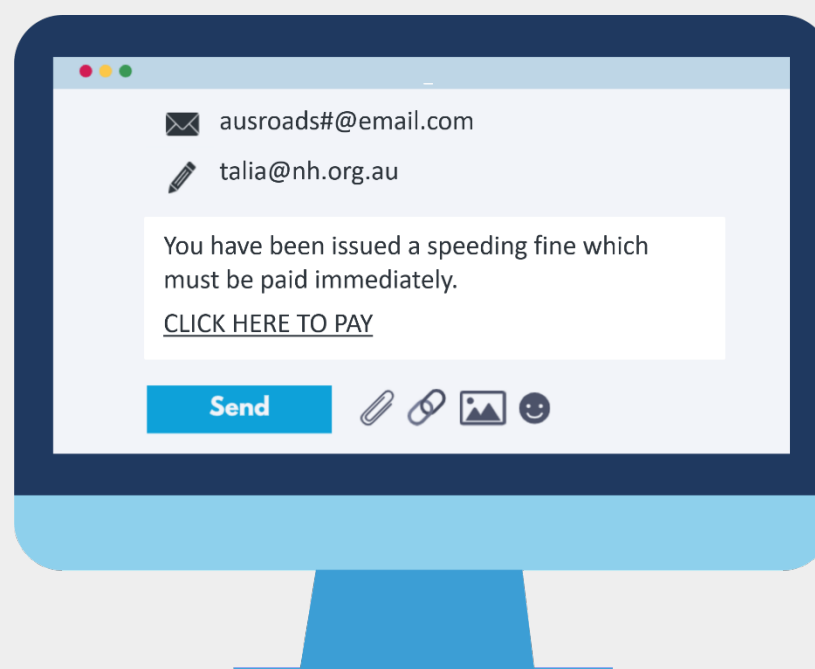
Generic greeting

Content appears in an image

Contains high risk attachments such as file types like .exe, .scr, .zip, .com, .bat

Missing details about the sender

Your email address appears in the 'From' address



The information appears too good to be true

For more information about phishing, visit the [ACCC Scam Watch website](#).

We're here to support you!

The [ICT Service Desk](#) is available to discuss any concerns you may have about cyber safety at Northern Health. Here's how we can help.



Reporting a security incident

Contact the [Northern Health ICT Service Desk](#) immediately if you have any concerns, need advice, or need to report a cyber security incident including any of the following:

- ☒ Data breach (for example, a lost USB with work data, or accidentally sending an email to the wrong person)
- ☒ Stolen password or passphrase
- ☒ Lost or stolen Northern Health device or equipment
- ☒ Phishing attempt, whether it was successful or not
- ☒ Inappropriate access to information.

Support for a phishing attempt

If you think you have been phished, notify the [Northern Health ICT Service Desk](#) immediately and be prepared to answer the following questions:

- ☒ What was sent to you and from whom?
- ☒ Did you click on the link provided in the suspicious message?
- ☒ Did you provide any information after clicking the link (for example, your Northern Health user ID and password)?

Advice about using portable storage devices

Contact the [Northern Health ICT Service Desk](#) for advice on protection and virus scanning for any portable storage device you may be considering using.

