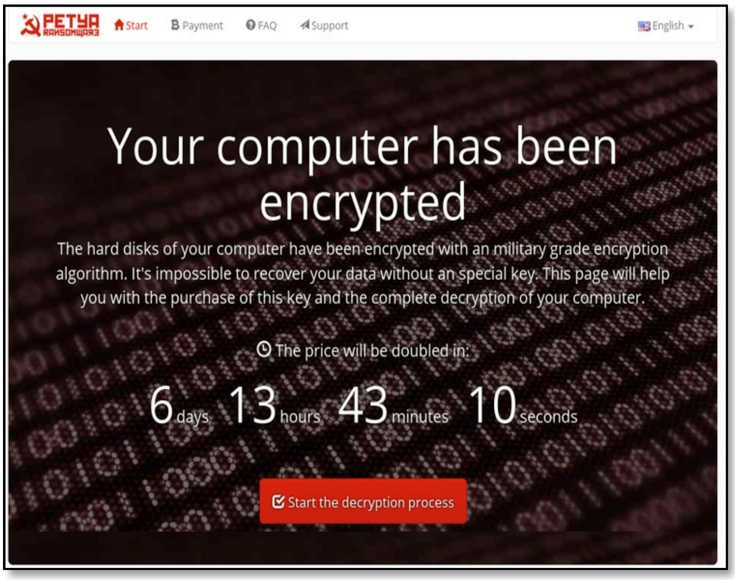
Cyber Security in 2023

a little CRC

Criminal activity can reach you even in the Australian bush…

Ransomware Infections…

Ransomware will infect your computer with malware (unwanted software) which leaves the computer running (sorta), but with all your personal data apparently lost or garbled and a message to pay a 'ransom' to recover your data.



Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

The price will be doubled in:

6 days 13 hours 43 minutes 10 seconds

Above: the Ransomware called 'Petya' demands payment.

Ransomware has infected some very high profile targets and, close to hand, the NCRC and the Bridgetown Shire Council. For the NCRC the solution was simple: we had an effective backup strategy. That allowed us to wipe the infected computer and restore all the missing data.

In the case of the Shire of Bridgetown-Greenbushes they, shamefully, paid the criminals' demanded ransom ($2,600). This is a sign that either their backup system wasn't working or they didn't have a properly tested way of restoring their systems using those backups. That was in 2018, but Ransomware is still a huge problem. We hear about occasional big organisations (like Medibank) falling victim to this problem and pay millions in ransoms, but in the meantime hundreds of individuals and small businesses are facing this every week.

Backups Are The Solution

What's the solution? In a word: backups. Backup your important data. If you're running a business you should also have a recovery plan. That's a plan for how you will go about cleaning your computers, changing passwords and restoring your accounts and data.

Backing up is different for everyone. The steps you need to take are:

1. Choose what data to include in your backup. What do you want to keep safe? It may be just important business files, or you may want to make sure all your photos, videos and old emails are safe.
2. Decide how to backup your data. You could use a cloud backup service or external storage devices.
3. Maintain a backup routine – daily, weekly or monthly?
4. **Check that your backups work – testing you can restore your data is a critical step, often overlooked.**

We have put that last point in bold because it is so often neglected. People buy an off-the-shelf backup solution and hope that it works without investigating how they would go about recovering their data in the event of a disaster.

What other perils are out there?

Despite all the changes in technology the main cyber-security threats remain the same as a decade ago:

Phishing. A hacker will try to get private information from you including your financial details. They do this by making fake internet forms/ websites, sending fake text messages or making phone calls in which they will pretend to be a company or government body and will ask you personal details such as bank account details, passwords etc.

To avoid phishing attempts, learn how to recognise a real website from a fake one (look in the internet address bar), and don't give out details unless you are the person who looked up the phone number and initiated the phone call.

Identity theft. Your details may be hacked, purchased, phished (see above), cracked or guessed. This can provide a hacker access to your accounts or personal details which they can use in various nefarious ways.

Overpayment scams. A (fake) company will contact you offering a refund. In the process they find incredibly subtle ways of ripping you off. Elderly and often very honest people are common victims of this scam type.

Invoice fraud, dating scams, trojans, keyloggers, viruses and worms. The list goes on…

How do I know I have a problem?

Some malware is obvious, threatening blackmail emails or pop-ups for instance. Other malware prefers to disguise itself.

The following signs may indicate there is malware on your computer:

- your web browser starts on a different homepage
- your files are inaccessible
- random error messages appear
- new programs, toolbars and icons have been installed

For more info visit Northcliffe CRC or go to www.cyber.gov.au

Monday, Tuesday, Wednesday 10am to 5pm | Thursday, Friday 10 am to 6pm

Northcliffe Community Resource Centre
www.northcliffe.org.au

Tel: 0455 438 890
PO Box 133
Northcliffe 6262
ncrc@northcliffe.org.au

We are a not-for-profit organisation supported by the Northcliffe Community and the Government of Western Australia

GOVERNMENT OF WESTERN AUSTRALIA
Department of Primary Industries and Regional Development