RANSOMWARE QUICK REFERENCE

Report suspicious activity immediately to David or Jason	
Phone: 03 9038 8188	Email: helpdesk@youritcrew.com.au

1. Is a Ransomware attack occurring?

Most common indicators include:

- An inexplicable slowdown in workstation or network activities
- Any suspicious changes to files, file names, or locations
- Unauthorized or previously undetected extraction of data
- Unrecognized or otherwise out of place file encryption
- Explicit splash screen messaging indicating an attack

2. Isolate the affected system or device

In the event of an ongoing ransomware incident where files are being encrypted, it's crucial to take immediate action to minimize the damage and prevent further encryption.

Here are the best steps to take right away:

a) **Isolate the Infected System**: Disconnect the affected device from the network to prevent the ransomware from spreading to other devices.
b) **Shut Down the Infected System**: Turn off the compromised computer to stop the ransomware from encrypting more files and do a hard shutdown by holding the power button or removing the power cord.

3. Check all other systems and devices.

Examine all network-connected devices and systems to ensure the ransomware has not spread beyond the initial device.

Take note of all systems you believe have been compromised and follow step 2 above to disconnect or remove it from the network.

4. Contact us again and wait for further instructions.

The incident response team at Your IT Crew will guide you through the next steps to resolve the issue.

Be aware that we may need to wipe the device hard drive and reinstall the Operating System (OS), cut off your cloud storage, restore your files from backups and reset your passwords depending on the severity of the attack.

It's important to stay vigilant

- Always thoroughly check messages and emails you receive
- Avoid links that ask you to log in or reset your password
- Steer clear of suspicious or untrustworthy websites
- Use a password manager to store unique and complex passwords
- Turn on multi-factor authentication

YOUR IT CREW