So, you've been held to ransom?

Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so that you can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files, or to prevent data and intellectual property from being leaked or sold online.

NEVER PAY A RANSOM

There is no guarantee your files will be restored, nor does it prevent the publication of any stolen data or its sale for use in other crimes. You may also be targeted by another attack.

Here are the simple ways you can remove ransomware, recover your files and protect yourself against future attacks. **If you get stuck, find a professional to help you work through a ransomware attack or call the Australian Cyber Security Centre's 24/7 Hotline on 1300 CYBER1 (1300 292 371).**

RESPOND TO A RANSOMWARE ATTACK

STEP 1	**Record important details.**	As quickly as possible, record important details about the ransomware attack. Take a photo of the ransom note or any new file extensions you have noticed.
STEP 2	**Turn off the infected device.**	As soon as you have finished Step 1, turn off the infected device by holding down the power button or unplugging it from the wall. This is the best way to stop ransomware from spreading.
STEP 3	**Disconnect your other devices.**	If there are other devices on your network, you should turn them off too. Start with your most important devices that store valuable information such as servers, computers, phones and tablets.
STEP 4	**Change your important passwords.**	Some forms of ransomware steal your passwords. As a precaution, you should change the passwords for your online accounts, starting with your most important accounts first.

RECOVER FROM A RANSOMWARE ATTACK

STEP 5	**Recover your information.**	Check your backups for use in Step 7. Make sure not to connect your backup to the infected device or network. If you think your backups may be infected with ransomware, or you don't have a backup, ask an IT professional for support.
STEP 6	**Remove ransomware from affected drives and devices.**	For most people, the best way to remove ransomware is to wipe all infected drives and devices and reinstall their operating systems. We recommend following this step for all drives and devices that were on the same network as the infected device at any point since the infection.
STEP 7	**Restore your information.**	After removing the ransomware in Step 6, it is safe to restore your information. Use the backups from Step 5, but only if you are confident that they are free from ransomware.
STEP 8	**Notify and report.**	If your business holds sensitive information or is part of a government supply chain, you may need to report the incident to regulators. Consult with oaic.gov.au. You should also report the incident to the ACSC through ReportCyber at cyber.gov.au.

PREVENT FUTURE ATTACKS

STEP 9	**Prevent future attacks.**	The ACSC has published advice to help you protect yourself against ransomware attacks, available on cyber.gov.au.

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre