SOUTH WEST POLICE
RCCU
Regional Cyber Crime Unit

Protecting against Ransomware

Ransomware is a malicious software which locks your device or data, and demands a payment to have it unlocked. It affects both organisations and individuals, and is a common way for criminals to cause disruption and financial gain. This advice can help you protect your devices from ransomware, and recover should you suffer an attack.

Backups

Backing up your data is a key defensive measure against ransomware.

What?

Identify what data is important to you. This would be anything you would be upset or inconvenienced to lose (e.g. photos, music, calendar appointments, emails).

Where?

You can store your backups on a physical device such as a USB drive, or upload to the cloud, whichever works best for you. If using a physical device, always unplug it once you have completed the backup - if you leave it plugged in, ransomware may lock your backups as well!

Auto-backup: Consider an automatic backup system, so data is automatically backed up on a regular basis, without you having to remember to do it.

Test & Check: Once you have regular backups in place. take the time to check and test them. This involves periodically checking what data is saved to the backup, and testing your backup file restores correctly on a separate device

Updates

Updates provide security patches against known weaknesses.

Install software updates on computers, mobile phones and tablets as soon as reasonably possible.

When you finish with your computer, simply select 'Update and Shutdown'. Phones and tablets can often be set to update overnight when you're not using them.

Apps

Only download apps from the genuine app stores, never from a website.

Apps from untrusted sources could contain malicious software.

Also, as with devices, ensure you update your apps when required. Many devices provide an 'auto-update' option which will automatically update apps for you.

Emails

When dealing with emails, always watch out for phishing attempts.

To avoid getting caught out, you should:

- Check that the email makes sense
- Never be scared to contact the person/company who sent the email to check it's genuine by calling a number you know is correct.
- Avoid clicking on links and attachments in emails, **unless 100% sure they are genuine**. Instead, try and find another way. For example, if you get an email from your online bank, don't use the link, and go to the bank's genuine website or app and log in there.

For more information on how to defend against Phishing attacks, please refer to our Phishing Advice Sheet.

Antivirus

Antivirus software protects your devices from malicious software, such as ransomware and other viruses.

Ensure that you have a reputable antivirus on all computers, mobile phones and tablets.

Regularly run scans and apply updates when available.

If you've been infected

Law enforcement don't encourage, endorse, or condone the payment of ransom demands. There is no guarantee that your data or computer will be unlocked.

Instead we recommend that you take the following steps...

1. Immediately disconnect infected devices from all network connections. Then reset your credentials (including passwords), and safely wipe the infected devices and OS.
2. Restore you systems from a trusted backup, and connect devices to a clean network to download/install the OS and other software. Install, update and run antivirus software.
3. Reconnect to your network. Make sure to monitor any suspicious activity, and run antivirus scans to identify if any infection remains.

Contact **Action Fraud** on 0300 123 2040, or through their website https://www.actionfraud.police.uk

For more information on protecting yourself against ransomware and malware, see the National Cyber Security Centre (NCSC)'s guidance at https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks