



THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON

Backup Data

Disaster can strike at any moment, whether it's a cyber-attack, flood, fire or accidentally dropping your device. If your entire business is saved in one location, it can all be lost in seconds. Ask yourself, how long can your business survive without access to your data and assets? Create a backup policy to prevent accidental loss or damage to your data. You can quickly recover from an incident and continue business as usual. Store your backup, off the wi-fi you connect all your devices, to avoid contaminating your files with malware. Use different storage methods, for the possibility that one may be compromised. Ransomware can infect backed-up data before you are aware of its presence, so you cannot recover from the attack. Regularly restore your backups so you know they are fit for purpose.

Where you Can Store your Backups

External Hard Drive

A physical device to store your data. This can be connected into the USB port or over Wi-Fi. Keep this stored in a secure location out of the office. Make sure the device is encrypted and can be locked with a password.

Encrypted USB Device

A physical device to store your data. Keep this stored in a secure location out of the office. USBs are easily lost or stolen, making your backups vulnerable if it is not stored appropriately. Make sure the device is encrypted and can be locked with a password. USBs do have limited storage space compared to other backup methods but they can still be useful to protect a select number of files.

Cloud Storage

A third-party online service to store your data. Windows and Apple products also have built-in backup capabilities. They provide:

- Large amounts of storage space depending on the package you choose.
- Recent file versions can be backed up automatically.
- Backups can be accessed from any device.
- It's a digital copy protected from natural disasters.

When selecting cloud storage make sure it is supported with updates, you can enable 2-step verification and your files are encrypted (protecting your data from unauthorised view. "At rest" means while they are stored and "in transit" means while you upload, download and move files). Use a strong password to secure your account.



@London_CRC



Cyber Resilience Centre for London



@CRCforLondon



londoncrc.co.uk



info@londoncrc.co.uk