What Parents & Carers Need to Know about

DATA BACKUPS AND STORAGE

Making backup copies of files and other content is very useful for avoiding issues (such as hardware failure, software problems or accidental deletion) that could cause the loss of important information or treasured images and videos. While backing up files is considered good practice, it's also essential for adults and children alike to stay aware of the risks which can potentially result from saving these extra copies of your info – particularly if your additional backup versions use cloud storage services.

BACKUP BASICS

Consider how valuable different types of files are – and what the impact would be if they were lost. Family photos and videos might be irreplaceable, for example, whereas emails to friends tend to be less important. This thought process can help you decide what to back up.

*For your most indispensable files, follow 'the 3-2-1 rule': keep **3** backups of your data (your original plus two copies) using **2** different media (such a USB flash, cloud storage or a hard disk drive) with **1** copy held in a physically separate location. This reduces the chance of a single event meaning that your files aren't recoverable from <u>any</u> of these backups.*

WHAT ARE THE RISKS?

DISAGREEABLE DUPLICATES

Because we tend to back files up in groups rather than individually, it's very easy for some content to get inadvertently swept up in the saving process – creating a duplicate that we aren't aware exists. If this were to include the unintentional backup of malware files, it would mean when we recover our data from the backup, we're also restoring the harmful malware to our computer, phone or tablet.

HIDDEN IN THE CLOUD

It's not unknown for children and young people to make use of cloud backup services to effectively 'hide' content that they know their parents and carers wouldn't approve of (such as something age inappropriate, for example). They can then delete the content from their device, safe in the knowledge that they can easily retrieve it from the cloud at a more convenient moment.

THE WEAKEST LINK

If any of our backups are insecure, then – in the event of a breach – the entirety of our data might become accessible to cyber criminals or other malicious individuals. Cyber criminals are aware that, by default, backups tend to contain important or valuable files that people want to keep safe – which makes them a popular (and potentially lucrative) target for cyber-attacks.

RANDOM RECOVERIES

When restoring data from one of our backups, we may find that some data is recovered which we hadn't even realised had been backed up. This doesn't necessarily sound like a huge drawback – but it could potentially cause a problem if the files were sensitive or personal in nature and then (without us realising) suddenly become available on our devices, where others might see them.

Advice for Parents & Carers

BE ORGANISED

Try to keep on top of what backups you and your children have in place – including where your files are saved (to the cloud or an external storage device, for instance) and how they can be accessed. It can also be helpful to stay aware of what data *isn't* being backed up, which could save you the time and the stress of looking for something in your backup that was never actually there.

KEEP THINGS TIDY

Where possible, curate your backups by learning how to add or remove content selectively. The former will save you from having to carry out a complete backup on every occasion (which can be time consuming), while being able to prune individual files can be extremely useful if a small number of unwanted – or possibly sensitive – items have been copied over and saved accidentally.

PRACTICE MAKES PERFECT

Find out how to recover files and information from backups until you're fully confident with the process. You could help your child practice with their own (or less essential) files, so they're able to restore items to their device if they need to. It's intensely frustrating knowing that your (or your child's) important files or cherished photo albums are there somewhere, but you can't get to them.

SCRUTINISE YOUR SECURITY

It sounds like obvious advice, but it's absolutely vital: ensure that your backups are secure. This includes appropriate technical measures – like encryption, strong passwords and multifactor authentication – and, where possible, physical security to prevent the media being stolen. If you're backing up to a hard drive or an external storage device, you should ideally use password protection.

Meet Our Expert

Gary Henderson is the Director of IT at a large boarding school in the UK, having previously taught in schools and colleges in Britain and the Middle East. With a particular interest in digital citizenship and cyber security, he believes it is essential that adults and children alike become more aware of the risks associated with technology, as well as the many benefits.

National Online Safety®

#WakeUpWednesday