Staying Safe Doesn't Get Any Easier

When it All Goes Wrong. Murphy's Law states, "Anything that can go wrong will go wrong." As all previous victims of this law know, it will also go wrong at the worst possible time. The only way to deal with this cataclysm in our lives is to plan for it.

OK, you've just become the victim of a *Ransomware* attack. Your documents, family pictures, virtually everything on your device is inaccessible. What will you do? You could pay the criminals responsible but you'd not be certain that they'd make things right. They *are* criminals after all. Or you might have backed everything up in advance, making the situation merely inconvenient instead of devastating. Even if you've merely had a computer failure, or a lost phone, your data will be at risk if you've not backed it up properly.

At this point, it's necessary to get (just a little bit) technical.

All common devices, including smart phones, tablets and virtually all computers provide mechanisms to back up your data and, to some extent, your operating system. The backup methodology falls into two general areas.

- Local backup
- Cloud backup

Local backup is exactly what it sounds like. You duplicate your data and keep it safe on an external drive. This can be done by simply copying or using a backup utility to do it for you. Since "thumb" drives are relatively inexpensive and some automatic backup programs are free, this is a solid option.

Cloud backup entrusts your data to others in the "cloud" which is somewhere as defined by the author's AI friend as "a network of servers, storage devices, databases, networking equipment, software, and other digital infrastructure that resides in physical data centers scattered all over the world."

Those who control the cloud tell us that our backed up data is perfectly safe and it generally is *except* when it all goes wrong. Not to frighten, but revisiting Murphy's Law, "What could go wrong?" Could the Internet fail?

So, which backup strategy should you adopt?

Since not mutually exclusive, why not both? Cloud storage usually works well, is usually safe and often free. Local backups give you control of your own situation and costs little, if anything. *Redundancy* in this context is a good thing.

The author, while not enthusiastically embracing the cloud backup approach admits to backing up critical data, including a lifetime of photos, to multiple external storage devices three times a week. Keeping backups not connected to the computer, e.g. thumb drives, is a good idea. Any device connected to a computer is vulnerable to damage caused by an online attack.

We mentioned **Ransomware** earlier. Another full frontal scam attack. Some are weak, like the one recently aimed at a relative's small business. The email read something like, "Unless you send $3,000 in Bitcoin by tomorrow, we will ruin your reputation." Some are devastating, as MGM and Caesars can attest to. Vulnerabilities in their security systems were exploited, denying them access to their data, costing them millions. Did they pay the ransom? They won't say.

And, remember. **Don't talk to strangers!**

Any Comments, clarifications or questions should be directed to the author at jgf6217@gmail.com.
Written by Joe Fitzpatrick