Crossing the Digital Divide – Cloud Cushions

Joe Feigon

Editor's Note: Following is the second in a series of articles on Web use and computers, graciously provided by Joe Feigon, courtesy of the Mendocino County Observer. Thanks, Joe!

The rainy season is fast approaching, and it can be tough on electronics. Electronics of all kinds last much longer where the temperature is consistent, the humidity nominal, and the air clean. I cheerfully accept the fact my electronics may not live as long as they could, but I can't risk losing my work, nor can you.

It's important to back up "stuff" you can't replace. It's convenient to back up "stuff" you want in one place. Some things are inconvenient to replace, some impossible. No one wants bad news. Impossible happens. Understand and use the cushion of a Cloud, and avoid hearing the dreaded: "It's gone".

Online storage is easy, safe, and fairly seamless. If you're a Gmail user, upload some files to Google Drive, it's secure, only you can access it, and it won't go away if your laptop drowns. Dropbox is free if you use less than 5GB (ample for stuff you can't replace). Microsoft users can (if they haven't already) create an account on live.com, or outlook.com, or register with an existing email account provided you have Windows 8, 8.1, or 10.

Data "in the Cloud" is stored in huge data centers, where hundreds of "servers" track changes in client files, keep backup images of all those files, distribute active and backup libraries through massive, high-availability, redundant storage-area-networks. Security is managed on several levels: authentication servers validate user credentials and/or ssh-keys through a web interface. The authenticated user is given a valid session ID (behind the scenes), that will cripple any file transfer should there be a "man-in-the-middle" attack. Once authenticated, all file transfers (to/from) your Cloud provider is encrypted or transported through an encrypted tunnel.

The major storage providers (Microsoft, Amazon, Dropbox, Google, Apple) have serious equipment and brain power protecting their storage area networks. Most data stores are replicated between multiple data centers, just in case the West Coast falls in the Pacific. Your data, stored at Microsoft or Dropbox or Google or Amazon is safer against loss or theft then it is in your office, at your ranch, in your safe, or at Aunt Sally's flat in Queens, New York.

What's on your computer that you cannot replace? How big is that folder? Do you have a fiduciary responsibility for that data? Define what data can't be replaced; measure it, value it, and decide an appropriate archival period. Some things should be kept forever, some should be purged after time. Medical records, Legal Records, Public Records, Personal Records. Physical copies to a safe deposit box or fire safe, electronic copies to your private Cloud account. Got it?

More articles by Joe can be found on at: http://www.mendocinobroadband.org/crossing-the-digital-divide-by-joseph-feigon/