The

Broadcasters' Desktop Resource

www.theBDR.net

... edited by Barry Mishkind – the Eclectic Engineer

Bits and Bytes

Don't Die With Your Password, and Five Other Computer Safety Tips

By Barry Mishkind, BDR Editor and Publisher

[February 2019] Keeping your computer files secure, yet available, is essentially a balancing act. Here are some tips for keeping your system safe and secure from all sorts of problems.

Not so long ago a friend died rather suddenly. Among the many problems with which his family had to contend: only he knew the passwords to his email account and website server.

No, he was not one of those people who used "password" or "123456" as his password – a practice that almost ensures someone will eventually break into your system. Nor did he put a "post-it" on his monitor with the passwords or tape it somewhere on his desk. He used good password practices like those located here.

Perhaps a worse situation – not just affecting personal papers or family photographs - when Gerald Cotton died suddenly this past December, he was said to have solely held the password to some $136 million in crypto-currency. As of yet, no one has managed to crack the password of his laptop which held the encrypted password for the money.

In the end, his company had to file for bankruptcy.

These real-life situations remind us to review six practices every computer user should know about – and utilize.

PROTECT, NOT PREVENT

Let us begin with the sincere hope that you do not have an early demise.

On the other hand, what if you did have a fatal car accident today? Would your business partner or mate know how to access critical accounts, including your on-line banking and brokerage accounts? Or, would your family know what to do with your email, facebook, or other web access points?

The smart solution is to ensure that your key accounts and passwords are located in the same place your Will and Power of Attorney documents are stored. In fact, a complete listing of all your accounts and policies will aid your family in the event you are incapacitated or die.

What? You do not have a Will?

Really, now is the time to think about that, no matter your age – Cotton was just 30 years old.

WE SAID PROTECT, NOT PREVENT

Obviously, if the issue is that there is something stored on one of your accounts that you would not want others ever to see, now is the right time to move it somewhere that will die with you.

Enough said.

For sensitive materials, including your financial accounts, nominate someone you truly trust, include them in your Will or Power of Attorney, and make sure they know where to find the information if needed. Also, check with the institution to ensure the paperwork is in order to allow them access without major legal gymnastics (often, this means a "joint account with right of survivorship."

For most people, the best solution is to leave a sealed envelope with a trusted person (family attorney or your best friend?), to be opened only in case of death. (You will need to update such a letter every so often as you change passwords and/or accounts.) At least this way, your family will not have to spend days or months – or lots of money and stress – to access your accounts.

REALLY SAVING SOMETHING

Those of us still in the land of the living may occasionally need to access information from time to time that might have been sitting on our machines for five, ten, maybe fifteen years or longer.

But have you tried recently to read back information from a 5¼-inch floppy (or, if you have been at it a while, an 8-inch floppy)? For most, this could be a real problem, even if you have a drive capable of reading the media, because all things magnetic degrade over time.

Even if you have saved your data files to a hard drive, you still have to be cautious – any IT pro will tell you the only question about hard drive failure is when it will happen, not if!

BACKUP OPTIONS

That is the key reason why it is important to backup the backup.

The best way is to save key files in several places – though not on the same hard drive (yes, we have heard of backups being on the same hard drive!).

Possibly you have heard of the 3-2-1 Backup Rule: have three copies of anything important, in two different formats (hard drive, solid state drive, CD, DVD, etc), with one of the copies at another location, away from your site.

This is good advice, and exactly where you keep the backup is important.

Why? Just think for a moment about the fires in California, or the flooding caused by Hurricane Sandy in the Northeast, or that in the Carolina's last year.

If critical backups were merely located in a different office in the same building, or at a neighboring site, there would be a great chance that any such backups would be destroyed, too. And not only the business data – family records and pictures easily could be destroyed.

FIND A GOOD PLACE

When looking for safe place for backups, many broadcasters have a built-in alternate site: the transmitter site. For example, mountain sites usually can be considered flood-proof.

Another option is to use the services of a data center. Generally, they have multiple power sources, UPSs, and plans to survive any local disaster short of a nuclear attack. Virtbiz.com in Dallas is one such data center that we recommend. In addition to a solid backup plan, they have multiple sites, including a tall building.

Depending upon the value of your data, a few dollars a month might be well worth it for the safety and security of those business records, picture files, and more.

By ther way, do spot check your backups from time to time. If you have been copying corrupted files over corrupted files or onto CDs that have rotted and gone bad, there may be little to recover later on. Finally, as new forms of storage appear, consid-er using them for some of your backups.

AVOID COMPUTER KILLERS

Most broadcasters naturally cringe when a lightning storm approaches. This is because even if a station strives to employ a good ground, surge protectors, and static dissiapators, there is always a chance that a direct lightning strike will happen and blast everything.

It is Murphy's Law that dictates *the most critical – and hardest to repair – gear is the one*

that will get smoked at the worst time. Possibly you may have survived many a storm with your computer online and not had any failures.

On the other hand, it could be the very next storm will take out your power supply or something on the motherboard.

The basic, first-line solution for power surges is easy. Just go to the local office supply or hardware shop and get a power strip with surge protector for five or ten bucks. Then, get something a bit more sophisticated,

UPS units and larger surge protectors are really cheap insurance (Often it is not so much the machine, but the data that is of value), Just be sure you do not leave yourself open for the disappointment of a computer that suddenly becomes a lump of dead silicon.

FIREWALLS AND ANTI-VIRUS APPS

Here is another computer safety tip many forget to put into practice: use an anti-virus program and pay attention to your firewall.

At least twenty years ago, the computer magazines showed how a computer hooked to the Internet without a proper firewall was *compromised in seconds* by hackers. Yes, seconds. And it is no better today.

All over the world bad guys are running scripts testing IP addresses one after another – and they do know where the cable company IP blocks are located for easy pickings. The results are some of the 'bot-nets' often used to attack servers and Internet sites.

There is a free firewall built into Windows, but *it needs to be turned on*. Other firewalls can be found on the Internet, some of them free of cost.

Another option is a suitable router, which will serve as a "gate" to anyone trying to "knock on your door." A WiFi router will often give you two features for the price of one.
Regarding anti-virus programs, most computers today come with one or more 30-day trial editions of anti-virus (and sometimes firewall) programs. Also, most Internet providers also offer a free AV program, Unless you – or the weekend staff (!) – habitually visit sites featuring suspect materials, many of these should protect you quite well, at no cost other than to load the updates regularly.

DO UPDATES – BUT CAREFULLY

Speaking of updates, do install them – although with certain exceptions.

One dividing line generally is whether or not the computer is connected to the Internet. Mission critical systems can – and should – live on the maxim of "if it isn't broke, don't fix it." In other words, unless you need some new feature, systems that are doing everything well can just stay operating that way, without the updates.

In contrast, systems that regularly connect to the Internet should be updated with the latest security patches to protect you from the bad guys and their attempts to break in or plant viruses or Trojans.

Unfortunately, the number of updates can sometimes become annoying, as are the practices of some companies.

Each time you download some company's patch you have to look and reset the radio button or you will enable automatic downloads at their desire. Most competent IT people select the "alert" status for updates so they can decide whether to download and update the computer or not.

The idea is this: more than a few times an update has actually created more problems than it solved. Therefore, when you get that message "updates are available," you might want to wait a day or three to see if the company needed to correct their update.

Another reason not to allow automatic updates is how an automatic update *may come down and reboot your computer in the middle of the night*, either deleting any work not saved or even interrupting the program automation.

ANTI-SOCIAL EFFECTS

Finally we would like to share a warning related to our "Connected Age."

Social media has become such an addiction to many, who post all sorts of details of their lives on facebook, Twitter, etc, details that could come back to create problems for them.
This is not just referring to the "I had a hamburger here at Woofie's in South Somewhere" type of posts. Rather, telling the world where you are and what you are doing could indeed come back on you in ways you do not anticipate.

For example, telling online "followers" that you are on vacation may not be such a good idea. Bad guys could be following you, too, and know exactly when to visit your empty house. It is not hard to search Twitter for "vacation," for example, and find names, then get addresses – and even maps to your door – on the Internet.

You think not? Perhaps you think not much information about you can be found? This short video should give something to think about.

Furthermore, as you no doubt have read, many social media sites have been hacked and personal information has leaked out. Worse, it could happen to an elderly relative alone at home.

Although we live in a world of "instant gratification," it might just be the course of computer wisdom to announce your vacation and those great photos after you return.

In conclusion: as the guy on TV says: "Be safe (and alive) my friends."

- - -

Would you like to see more articles like this one? Just sign up for the BDR Newsletter. It comes to you one-time-a-week, and does not flood your inbox. It takes only 30 seconds to sign up!

- - -

Return to The BDR Menu