Author Login

HOME   ABOUT   ENDORSED BOOKS   THE ENDORSEMENT   SUBMIT   BLOG   CONTACT

| Latest Endorsed | Irresistible Collection | Blog | Latest News |

WE'VE ENDORSED MORE THAN 100 BOOKS
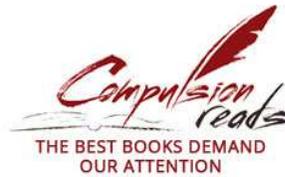
Compulsion reads
THE BEST BOOKS DEMAND
OUR ATTENTION

Safe Data Practices For Writers

Posted on November 12, 2013 by Jessica

Note from Compulsion Reads: On this blog we often like to dig into the mechanics of writing, like how to develop strong characters, avoid info dumps and keep grammar errors and typos at bay. Sometimes, however, focusing on the mechanics has nothing to do with what goes on inside the story and everything to do with how you protect your writing from computer failure, viruses and other outside threats. In this helpful blog post, author John W. Nichols shows you how to keep your precious works in progress safe. This is a must-read for any author who doesn't want to experience the excruciating catastrophe of a lost file.

What would you do if you lost your WIP and couldn't get it back?

Guest Post By John W. Nichols

How did writers like Mark Twain or Ernest Hemingway crank out so many books without a computer? Imagine the pain of writing, rewriting and editing using only pen and paper. No thanks! I love my desktop PC, my laptop, my writing tools, and instant access to worldwide data. Am I spoiled, lazy, or simply maximizing the available resources to write smarter?

We rely on computers, smart phones, and tablet devices for everything from paying our bills to expressing our opinions. As a writer, I have several works in progress, a collection of notes, and a number of idea files which may lead to future best-sellers. As an engineer, I question the security of my data. I'm not worried about someone stealing the plot from my latest novel or quoting me without proper credit. The more feedback I receive on my writing, the better. I'm concerned about losing my laptop or having my hard drive crash. Then what happens to all those files?

Writers, we need to stop the flow of ideas long enough to ask a practical question, "If something happens to this electronic device, can I recover my work?" Let me suggest 3 steps we can take to protect our all-important writing data.

1. Develop a data backup plan.

For years I copied files onto DVDs or memory sticks I stored in the desk drawer. I prided myself on having protected my crucial data. If I corrupted a file, suffered a hard

Categories

Daily Writer Inspiration (136)

For Readers (39)

For Writers (59)

Daily Writer Inspiration

I finally had everything I'd ever wanted. I was exactly where I wanted to be. So Why couldn't I just enjoy it?

Writer's Prompt

drive crash, or purchased a new PC, I could easily locate and restore my work. This scheme has a glaring deficiency, though.

What happens if a fire, tornado, or hurricane destroys my home? If the computer is destroyed, will my backups, hiding 3 feet away, survive? I could deposit the backup media in a safety deposit box at the bank, but that is inconvenient.

Many newer computing devices have no local drives. Users must venture into the cloud and use Google Drive or some other service to manage data. Why not let Google worry about backups and focus on the writing? There are pluses to cloud computing, such as streamlined collaboration, but I use Scrivener, Gimp, Picasa, and a host of tools not yet built into the cloud. For me the solution is not yet practical.

Writers should consider a backup service such as Carbonite or ZipCloud. The vendor's software is installed and configured, making backups automatic. I can focus on my writing, knowing my files are being encrypted and archived on the vendor's server miles from my home.

2. Virus protection is a must.

My research often takes me to unfamiliar web sites, and some are baited traps waiting to snare unsuspecting surfers. Viewing the site without protection may allow installation of a virus or spyware on my system. Perhaps the hacker seeks my email address book so he can flood my contacts with spam. Maybe the virus is more destructive and zaps my entire hard drive. Either outcome is unacceptable. The expense of a virus protection package is the price of admission for healthy networking. Norton and McAfee are two well known products, but there are others. Please, writers, if you connect a device to the web, assume it can be hacked and protect your data as well as you can.

3. Be password smart.

As the number of our accounts and passwords multiply, we struggle to recall them. I used to keep a written log of passwords and reused the same password for many online accounts. Neither practice is secure.

Business Week[1] reports it takes a hacker 10 minutes to crack a lowercase password that is 6 characters long. Use an 8 character password that mixes lower case, upper case, numbers, and symbols, and the time to crack jumps to 463 years.

A password management system can ease the pain. Norton includes Identity Safe in some packages and shareware password managers, such as Password Safe[2], are available. With Password Safe, my easily-remembered 19 character string unlocks access to my encrypted password and account information.

Writers, our identity, personal data, and work in progress belong to us. We need to review our protection practices and consider the integrity of our password and backup strategies. Investing in good habits now may easy the pain of recovery should tragedy strike.

<div align="center">***</div>

John W. Nichols is the author of *Go For The Gold: Honch Wilson Adventure #1,* an action-packed novel for tween readers that has earned the Compulsion Reads quality book endorsement.

John W. Nichols writes from Raleigh, North Carolina, where he lives and gardens with his wife. John is a professional engineer who has authored mounds of technical documentation during his 30 year career. He now writes full time for his readers. Learn more at: http://www.nicholsnotes.com

---

[1] Source: http://www.businessweek.com/magazine/content/11_06/b4214036460585.htm

[2] Available at: http://passwordsafe.sourceforge.net/

This entry was posted in For Writers and tagged Computers, data backup, Files, Passwords, Virus protection. Bookmark the permalink.