

Protect your documents from digital thieves

Last week we covered the numerous versions and editions of Microsoft Office that have been produced and released over the years. Though I'm writing this column with Word from MS Office 2003, sometime this year I plan to upgrade



John Deans

all the way to Office 2010 by-passing the current Office 2007 that has been on the market for a few years.

Like others, my digital work is primarily in Outlook for email, Excel for spreadsheets, and Word for word processing. I even still surf the Web mainly in MS Internet Explorer so I can easily toggle between secure financial sites and non-business related sites. The only other non-Microsoft application I spend significant time working in is Intuit's Quickbooks to manage my company's finances.

To safeguard my hard work the first and foremost chore is to back them up onto multiple media. We have covered backups numerous times, but just to touch on it I have all my data automatically copied to external hard drives and uploaded to both

DataDepositBox.com and Carbonite.com.

That is a three-layered redundant recovery system that runs every night to protect my digital assets from hardware failure, theft, or God forbid, fire.

For those really important and high security level files like password documents and bank account spreadsheets, I have internal file protection implemented on them. This is in case my system is ever compromised, an e-mail attachment is intercepted or backup files are stolen.

Thieves in Washington Coun-

ty are in high gear breaking into people homes and stealing their guns, TVs, cash and computers. I hear about this all the time due to having the sheriff's department as a client and being president of Crime Stoppers. If ignorance is bliss, I sometimes wonder what it would be like not knowing the frequency and increase of county crimes on a daily basis.

The other big threat that is also on the rise is identity theft. Once a year when a shooting buddy from Houston comes to our ranch, he brings along a big box of personal and financial papers to be burned. After our ammo is exhausted at my range, we have a few beers and burn his box of paper liabilities.

This guy is so thorough he does not trust shredding, and burning household trash in Houston is frowned upon.

For those sensitive and financial files that contain private information you need to secure

them electronically. This goes double with spreadsheets and documents that contain details about your identity like bank account numbers, online passwords, or your social security number.

Numerous times I have been reloading data back onto a client's computer and saw files called passwords.doc or accounts.xls. With obvious file names like that I had to quickly test their security by clicking on them to see if there were any protections on them.

Most of the time they would open right up with no security challenge at all. This would prompt a lecture to that client about critical file security.

This is like putting a box containing all your tax and banking papers labeled "Personal Finances" and leaving it out in the hallway of your home. Any thief would see that upon break-in, grab just that box and run. There would be no need to take any other item in the house since that personal information represents a goldmine and the ability to steal much more from their victim over a longer time with little chance of ever being caught.

There are a couple of ways to secure your files individually. One way is to put a password on the file which from that point is required to open and view the document. Another and even more secure way to protect your critical files is to encrypt the data using a password as the key to decrypt the data.

Let's say you are one of those yahoos that keep all their online passwords in a file called Password.doc with Microsoft Word. First of all try to be a bit less obvious and use a random filename other than Password.doc and call it something like aAj-3J11aajb.doc. This would float to the top of the alpha-sorted list under MS Explorer so it would be easy to find but would not be obvious to data thieves if they got hold of your PC or backup hard drive.

Now that you have used a more secure file name rather than one that says, "Come pilfer me by opening this file now.

doc", you need to lock it up. Under MS Word 2003 click on Tools -> Options and then the Security Tab. From there you can enter a password in the "Password to open:" box which will both set the password and encrypt the file.

Excel 2003 works the same way to set a password. Use the procedure above to secure your spreadsheets with critical data in them. All of my company financial Excel files are password protected and digitally encrypted just in case one gets loose.

Make sure to use a good password that is at least seven characters, has both upper and lowercase letters, one or more numeric's, and throw in a special character or two. The stronger the password the more secure the file. Please for the love of Pete, do NOT use 'password' for the password since all data burglars try that one first.

Under the new Office 2007 GUI (Graphical User Interface) within MS Word and Excel you click on the main round Office button at the top left, then on Prepare and choose Encrypt Document. Use those same strict password requirements when you type in your password which acts as a key to decrypt the file and open it to see its contents.

If you even need to pack and secure numerous files in a single operation then download and purchase WinZip for around \$30. WinZip will enable you to create a single archive file containing multiple files that is both encrypted and password protected.

Bottom line: When you have files containing secure data, be a paranoid as my Houston buddy by password protecting and encrypting those files to deter digital thieves.

Next week's column: Technology and shooting.

John Deans of DeansConsulting.com is a Brenham area computer networking consultant who can be reached at 289-2233 or John@DeansConsulting.com for questions and comments.