

Title:

Is Your Data Encryption Really Secure

Word Count:

1521

Summary:

An article about various types of data encryption and how you might have a false sense of security.

Keywords:

Data Encryption, File Encryption, Folder Encryption, Volume Encryption, E-mail Encryption

Article Body:

How Do You Know Your Data Encryption is Really Secure

-----  
There are various types and methods of data encryption. Some of the most popular forms of data encryption are file encryption, folder encryption, volume encryption, and email encryption.

The Windows XP operating system has the ability to perform file and folder encryption. There are several different types of encryption available in Windows XP.

If you routinely deal with confidential or sensitive information, or if you are concerned about the security of your data, you should consider using encryption.

First, What Is Data Encryption

-----  
Throughout ancient and modern history people have come up with ways to mask, hide, and verify the authenticity of their communications.

Encryption today is much more advanced and complex. It is used for everything from securing military communications to protecting your personal information.

Most Data Does Not Start Out Encrypted So Be Careful

-----  
The primary reason I am writing this article is to point out a couple specific issues with data encryption that you should be aware of.

Let's take for example, a word document that contains your personal financial information. You have just finished writing the document and you hit the save button.

While you were writing that document, you probably hit the save button several times. Or if you are using a word processing application that automatically saves your work, you may not even realize it.

Now that you have finished your document and copied or moved it to the secure folder, your document is still not encrypted.

Changing The Location Of Unencrypted Temp Files

-----  
The primary way applications like Microsoft Word determine where to store temporary versions of your documents is by using a set of default file names.

Encrypted Files May Not Stay Encrypted When Copied or Moved

-----  
Another thing you should be aware of is what happens to encrypted files or folders when they are copied or moved.

Make Sure Deleted Unencrypted Files Are Really Gone

-----  
Because data that is deleted from disk may be recoverable for quite some time, I use another program to delete files.

Conclusion

-----  
If you are concerned about keeping important data confidential, file, folder, or disk encryption is a good idea.

You may reprint or publish this article free of charge as long as the bylines are included.

Original URL (The Web version of the article)

-----  
<http://www.defendingthenet.com/NewsLetters/IsDataEncryptionReallySecure.htm>

This is a demo version of txt2pdf v.10.1  
Developed by SANFACE Software <http://www.sanface.com/>  
Available at <http://www.sanface.com/txt2pdf.html>