



BackupSoEasy™ Online Backup Whitepaper What is encryption, and why use it?

Encryption is the act of turning a block of plain text or other raw data (such as binary computer files) into "ciphertext," encoded blocks of text. There are a variety of software packages available today which leverages the processing power of modern computers to bring encryption to bear on a number of tasks. Modern computer encryption systems use complicated techniques developed over a number of years, and are able to provide an advanced level of security. Most encryption experts believe that with the correct configuration and options, today's encryption software can generate encrypted text which can not be broken by even the most sophisticated attacks.

Encryption Applications:

Browsers:

Most users have probably already used encryption in a web browser. Modern e-commerce web sites support an encrypted connection to allow consumers to safely submit credit card numbers and other sensitive data. Many OSU sites offer this security as well: [OSU Webmail](#), [Buckeyelink](#), and [Carmen](#) are just a few of the many sites that do so.

Email:

The original design of electronic mail did not make any allowances for security. As email has evolved into a mass medium, users have begun to use two solutions to existing serious problems with email security.

- **Authentication:** Email services rely on the person sending an email to provide his/her own identity -- i.e., they only pass along the email address that a message claims to be "from." It is extremely easy for anyone to change this address and send messages that claim to be "from" someone they are not. Most



BackupSoEasy™ Online Backup Whitepaper

What is encryption, and why use it?

current users of email have experienced the frustration with large amounts of spam originating from forged return addresses -- or even discovered that their own addresses have been forged as a source of spam. This same vulnerability has allowed virus authors to pass viruses through email for many years, by making an infected attachment appear to come from a trusted source.

Modern encryption techniques allow an email to be digitally "signed" by a sender. The recipient of such a message can check a signature to determine that an email message actually came from the person claiming to be the sender.

- **Secure Transmission:** Email systems, by default, send messages in plain text. As a consequence, any person using a software package called a "packet sniffer" to "eavesdrop" on a network can easily read email messages being delivered over that network.

To put it another way, when you send an email message, you should think of it as a postcard readable by anyone handling email -- not as a letter inside an envelope. This clearly presents problems for anyone wishing to exchange sensitive information via email. Encrypting email messages offers a solution.

Storage of Sensitive Data:

Many modern professional computer users must manipulate data which could be considered sensitive. Doctors might store patient information. Brokers might store their clients' financial histories. Even home computer users might store personal information on their computers -- their own personal information. All this information is vulnerable to



BackupSoEasy™ Online Backup Whitepaper **What is encryption, and why use it?**

exposure in the event of the theft of the computer itself. This concern is especially acute for users of laptop computers. Even if the computer requires a password to start up, a thief can access the contents of the hard drive simply by connecting it to another computer. The only way to ensure the safety of sensitive data on your hard drive is to encrypt it. Some products can even encrypt the entire hard drive, providing an additional level of security at system startup.



Many thanks to Ohio State University for this public document



BackupSoEasy™ Online Backup Whitepaper

What is encryption, and why use it?