



Article Side

The four core elements of secure file sharing by [Emil](#)

Article published on January 2nd 2012 | [Internet](#)

As file sharing with file hosting services becomes more commonplace, it is important to understand the four core elements of secure file sharing that are necessary when you send large files online.

Authentication

The Internet is anonymous. So when you transfer big files to others, it is important to be able to verify their identity. This is called authentication, and there are an infinite variety of ways to accomplish this task. Perhaps the easiest way to authenticate the user is by using the email address of an existing email account. Email accounts are tied to the individual, and can be verified with a confirmation email. Confirmation emails serve two purposes. First, because they require user interaction, typically by clicking a re-direct link back to the website, confirmation emails help to confirm that the user is in fact alive and not an automated computer program. Second, people keep their email addresses for many years, which reduces the odds of your email being received by the wrong person. If the file sharing website protects the account with a password, this creates a core layer of security.

File Download Passwords

Password protection of files will add another layer of authentication for secure file sharing. File sharing sites that offer password protection will encrypt your file in such a way that it cannot be un-encrypted without the password. When you communicate the password via a method other than your primary communication channel (e.g. by using a phone call or text message), you are creating a key that greatly improves your security.

Secure Transfers

Once you have authentication established, you can begin uploading files to the file server. However, because the Internet is open by design, your large file transfers will go out over public Internet. Thusly, security of the file transfer is critical. Secure Socket Layer (or SSL) transfer protocols will encrypt your files as they are being transferred. If a malicious user somehow intercepts your communication, they will be only get scrambled data.

Encrypted Files

Once your file has been successfully uploaded to the file server of the file sharing website, it must be protected from hackers. If a hacker is able to penetrate the security of the file sharing website's file server, they will have full access to your files. Therefore, it is important for your files to be secure-at-rest. The American Encryption Standard (AES) is an encryption method that was developed by the National Security Agency to protect data that is in this vulnerable state. With AES encrypted files, a hacker that breaks into a file server will only get worthless scrambled data.

Conclusion

When a file sharing website authenticates users with secure logins, protects file transfers with SSL encryption, uses AES encryption to protect data at rest, and offers passwords to protect file downloads, any company or individual user will have sufficient protection to use the website for their big file transfers.

Article Source:

<http://www.articleside.com/internet-articles/the-four-core-elements-of-secure-file-sharing.htm> - [Article Side](#)

[Emil](#) - About Author:

The author is an expert in Internet file transfer services and has written several articles to help people find the right service to a [send large files](#) through the Internet. He has also written extensively on how to a [send large files](#) and the benefits to those who outsource their file hosting services.

Article Keywords:

file sharing, file share, send large files, free file sharing, file hosting, transfer big files, file upload

You can find more [free articles](#) on [Article Side](#). Sign up today and share your knowledge to the community! It is completely FREE!