The internet has made it easier for us to share important information with each other, whether it is related to our personal or professional lives. But if the information shared is not securely transferred to our intended receivers, it can cause breach of privacy or embarrassment that can take us a lot of time to recover from. It’s very important that whenever we are sharing or transferring any data online, it should be secured from intruders. The good news is that there are many ways you can ensure this. Additionally, there are also many tools that can help transfer data securely from a sender to receiver.

Let’s look at some of the best methods to secure the transmission of confidential or sensitive data.

**Email Encryption**

Many vendors today offer a range of products that can encrypt emails and ensure secure transfer of data. The receiver can also use the same encryption method from their end. This method is mostly web-based and works by sending the recipient a link, who then logs into a secure email-server after clicking it. From there the recipient can safely view the email message along with any attachments. The email server is either outsoudcee to a vendor or owned by the organization itself.

**Website Encryption**

This method of securing data is for businesses that collect sensitive customer data from their website. This holds especially true for ecommerce businesses that use customer’s cardholder data used for carrying out [online transactions](http://www.cardzgroup.com). The general practice to secure data entered in a website is to use a Secure Sockets Layer (SSL) for encryption, which allows secure transfer or data over the website. Though it is not possible to totally eliminate the security risks, you can greatly minimize the risk of data breach.

**File Transfer Protocol (FTP) and Secure File Transfer Protocol (SFTP)**

FTP is a standard network protocol that copies a file online from one host to another. SFTP or Secure FTP is one of the safest ways to transfer data online. By using these protocols, data can be transferred only after entering a username and a password. In order to use SFTP, you need to have access to a server, which can be either bought or rented. With the server in hand, you get a username and a password which can be used for uploading and downloading files. Majority of operating systems have incorporated FTP into their file explorers to allow users to transfer, copy and edit files on the server.

Before uploading the files, you can secure them by seting up a password. This step is important because even though the FTP connection is encrypted, the files are not.

**Secured Hyper Text Transfer Protocol**

HTTP is used typically to transmit hypertext files between a web server and a browser. The default settings of HTTP don’t allow it to carry out any data encryption or user authentication. To keep information transmission secure, you need to add encryption to HTTP, which is done by using Transport Layer Security or TLS. Secure HTTP or HTTPS as you may call it, is supported by most of the web servers. HTTPS provides server end authentication and allows the server to validate the client or use any authentication service.

**Off the Record Messaging**

Off the Record or OTR messaging is a feature for messaging platforms. OTR helps you encrypt messages before their transmission from your computer to any receiving computer. This ensures that you can send files to the receiver in a secure manner. You can also add further security and ensure that your communication is not being intercepted by using security codes that are provided with this feature.

**Cloud Services**

A cloud service is also a good method to securely store or share your files. A user can upload the file to a central repository from where other users can read or save the file to their device. The data is hosted on the cloud by a third-party, but you can specify the permission level for the receiver as read-only, download or edit. Dropbox and Google Drive are two such examples of cloud storage. Dropbox uses SSL/TLS for file transfer to ensure that the data remains secure. It makes a tunnel that is secured by 128 bit or higher AES encryption. The file data in Dropbox is stored in fragmented blocks which are not recognizable and highly encrypted. Additionally, a user can only view your files if you provide them with a link to view or edit your file.

**Peer to Peer (P2P) Communication**

A P2P file transfer does not depend upon a central server for hosting the data. Rather, clients are individually connected to a distributed peer network and carry out the data transfer over their personal network connections. P2P is a great method to securely share files within a small group of people.

**Near Field Communication**

Just like Infrared and Bluetooth, Near Field Communication or NFC allows safe file transmission for free. It was first used as a medium for making payments from contactless smart cards. NFC uses high-end encryption and special processors to secure file transfer. Though it is considered secure, it’s still advisable to turn off your device’s NFC when not needed as it can be misused as a host for criminals who can tap into files of other people with less secure NFC service.

**The Bottom Line**

Companies realize that it’s very important to get online protection these days. As security breaches and information hacking cases are increasing every day, it’s important to apply some or all of these secure methods when transferring data from one place to another and ensure your online safety.