Article published on February 17th 2012 | Internet

E-mail has become an indispensable communication tool for individuals and businesses. And many times, e-mails contain confidential and sensitive information that must be protected from eavesdropping. E-mail messages are often sent in clear text over the Internet without any encryption e-mail. Sending unencrypted messages over the Internet, like sending cards by post, everyone who has access can read or change its content.

While e-mail protocol used for sending e-mail over the Internet can support encryption, it has no reliable way to guarantee or provide end-to-end encryption. Even services such as Gmail, which support encryption between your computer and them cannot guarantee your message will be transmitted securely between your mail server and recipient's mail server. This is because if the recipient's mail server does not support encryption Gmail forced to return to the transfer of messages in text format. The same is true of virtually all personal and corporate media mail.

Perhaps even more disturbing is the copy of the message is typically stored on your computer is open, your company's mail server or host, a mail server for each recipient and each recipient's computer. During the message, usually takes a split second, as soon as your message is stored is usually sticks around for many years. It provides numerous opportunities for unauthorized access to e-mail and a legitimate concern of confidentiality. A good solution to encrypt e-mail will use the powerful techniques of cryptography to ensure your messages are stored and transmitted as reliably, and that only you and your recipients are able to decrypt the message.

Traditional solutions for encrypting e-mail require at least a moderate degree of computer expertise to implement. There is software to purchase, download and install. There are encryption keys to create, publish and maintain. And what do you do when one of the recipients using a variety of encryption technology from your own? Do you buy, download, install and configure their solution in addition to your own or you require them to buy, download, install and configure your solution?

If you use a locally installed e-mail program such as Outlook, you can protect your e-mail messages, download free secure add-on for Microsoft Outlook, which will allow you to send and receive encrypted messages in your Outlook account. There are other e-mail encryption service that allows you to send personal messages for free without downloading software or the use of encryption keys and works on any email client or web-enabled device.

If your mail is not encrypted, its contents and any subject read or change it. It is up to you to protect yourself and your data. Fast rule to follow is: data encryption, which would be problematic if others have access to it.

Article Source:
http://www.articleside.com/internet-articles/what-is-the-need-to-send-encrypted-emails.htm - Article Side

Brian Adams - About Author:
JumbleMe makes it easy to send encrypted emails and providing top quality a email encryption services. JumbleMe also provides best options for a hipaa compliant and a hipaa email. Scramble your email so it's almost impossible for anyone to break the encryption unless you give them the code. You can use any computer, even handhelds, any time, any place.

Article Keywords:
encrypted email, hipaa email, secure email

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