

## Secure Email with Encryption

Warren Peterson

Email continues to be the most used application on the Internet, surpassing web surfing, instant messaging, and other online applications. Virtually every person who uses the Internet relies on email as one of their core online functions. However, with this use of email, comes a risk. And, it is a risk that virtually none of the users of email are aware of.

There is plenty of attention given to the risk of a virus. People realize they have to use anti-virus systems. There is plenty of attention given to passwords. People realize they are not supposed to give their passwords out to strangers. However, with email, the risk isn't ever discussed.

When you send an email message, it is sent without any protection, and is sent in what is called, clear text. Clear text messages can be read by anyone along the path between you and the recipient. Your email message goes from computer to computer as it moves along the Internet, and if someone wanted to, they can read your message at each point on the way. Another problem is that anyone can pretend to send an email message as "you". A simple change in their email program settings and the email message will say it is coming from The President, - something called spoofing the source of an email message.

These risks can fall under one of two main categories, Passive Threats and Active Threats. Passive threats are those that simply involved a third party reading your emails, without authority. Active threats would be ones where a third party is trying to change your email, or pretend to send an email as you, from your email address.

The solution to problem like these is to use encryption. There are many different forms of encryption, and several solutions for email, with one of the most popular solutions called Pretty Good Privacy (PGP). PGP was created by Phil Zimmermann to address privacy issues dealing with transferring electronic information. As such, it became a natural tool to use in securing email.

PGP is available for commercial use from [www.pgp.com](http://www.pgp.com) and an international derivative is available from [www.pgpi.org](http://www.pgpi.org). PGP can be used on many different types of computers, so you will be able to find and download a version for your system.

When you decide to use PGP, you have a little bit of configuration to do before you can secure your email messages. PGP, and other forms of encryption like this, uses what is called public key cryptography. That means that you have a set of keys to lock and unlock, or encrypt and decrypt, your messages. To use PGP, you will make one of your keys public, allowing other people to use it.

Your configuration then will be in the creation of your keys. Thankfully the software helps you with this, and you simply have to answer some questions and create a

keyphrase (this is like a password). Once the software helps you create your keys, you can send your public key to all your coworkers, friends and family.

Now that your coworkers, friends and family have your public key, whenever they want to send a message to you that is secure, they will encrypt (or lock) the message with your unique public key and send it to you.

Once you receive the message, you now need to decrypt it, or unlock it. You have one more key (remember you made two with the software). This key is your private key, and you use this key to decrypt, or unlock, all the encrypted messages you see.

The overall process then is to install encryption software, such as PGP, have the software help you create two keys, one public and one private. You will send your public key to your coworkers, friends and family. Anytime they wish to send you a secure encrypted message they will encrypt (lock) it with your public key and send it to you. Once you receive the message you will decrypt (unlock) it with your private key and read the message.

Following this procedure, you will be able to exchange secure email that no unauthorized person can read or modify. Your email will remain private between you and those you wish to communicate with, no one else.

Eventually, one can expect that all email systems will move towards this type of technology. Until that happens, the risks to the number one application on the Internet will remain.

*Warren Peterson is the President and co-founder of Security Certified Program,  
[www.SecurityCertified.Net](http://www.SecurityCertified.Net)*