mindcentric
SINCE 1999

Why You Should Encrypt Your Email?

Why You Should Encrypt Your Email?

Many people suspect that security is mostly hype. You don't really need to bother with all those complicated passwords, antivirus software, firewalls and such. It's all just security software vendors and security consultants trying to scare everyone so they can sell their products and services.

There are common sense steps everyone should take to secure their computers and networks, but there is certainly no shortage of hype in the news. Like the latest hot mutual fund – by the time it makes it into a newspaper or magazine, it is old news and most likely too late for you to react to anyway.

However, as one of the common sense measures that aren't pure hype, you should consider encrypting your email communications. If you are on vacation you might send a picture postcard to a friend or family member with a quick "wish you were here" sort of message. But, if you are writing a personal letter to that same friend or family member, you would be more inclined to seal it in an envelope.

Why Should You Encrypt Your Email?

If you are mailing a check to pay a bill, or perhaps a letter telling a friend or family member that the extra key to your house is hidden under the large rock to the left of the back porch, you might use a security envelope with hatched lines to obfuscate or hide the contents of the envelope even better. The post office offers a number of other means of tracking messages – sending the letter certified, asking for a return receipt, ensuring the contents of a package, etc.

Why then would you send personal or confidential information in an unprotected email? Sending information in an unencrypted email is the equivalent of writing it on a postcard for all to see.

Encrypting your email will keep all but the most dedicated hackers from intercepting and reading your private communications. Using a personal email certificate like the one available from Comodo you can digitally sign your email so that recipients can verify that it's really from you as well as encrypt your messages so that only the intended recipients can view it. You can obtain your free certificate by filling out a very short and simple registration form.

That actually introduces an added benefit. By obtaining and using a personal email certificate to digitally sign your messages you can help to stem the tide of spam and malware being distributed in your name. If your friends and family are conditioned to know that messages from you will contain your digital signature when they receive an unsigned message with your email address spoofed as the source they will realize that it is not really from you and delete it.

How Does Email Encryption Work?

The way typical email encryption works is that you have a public key and a private key (this sort of encryption is also known as Public Key Infrastructure or PKI). You, and only you, will have and use your private key. Your public key is handed out to anyone you choose or even made publicly available.

If someone wants to send you a message that is meant only for you to see, they would encrypt it using your public key. Your private key is required to decrypt such a message, so even if someone intercepted the email it would be useless gibberish to them. When you send an email to someone else you can use your private key to digitally "sign" the message so that the recipient can be sure it is from you.

It is important to note that you sign or encrypt all of your messages, not just the confidential or sensitive ones. If you only encrypt a single email message because it contains your credit card information and an attacker is intercepting your email traffic they will see that 99 percent of your email is unencrypted plain-text, and one message is encrypted. That is like attaching a bright red neon sign that says "Hack Me" to the message.

If you encrypt **all** of your messages it would be a much more daunting task for even a dedicated attacker to sift through. After investing the time and effort into decrypting 50 messages that just say "Happy Birthday" or "Do you want to golf this weekend?" or "Yes, I agree" the attacker will most likely not waste any more time on your email.

Author Tony Bradley, CISSP-ISSAP

June 24, 2018