

The dangers of using email

Most people who use email are aware that there are dangers associated with it, yet there is one serious risk that many remain unaware of.

The two threats which people are most familiar with are spam and viruses. Spam is unwanted or unsolicited email and although it's often considered more irritating than dangerous, what it contains can be hazardous to you and your company. Spam emails can contain viruses, which may attack your internal systems in order to steal or destroy your data. They can even turn your computers and email servers into weapons of spam propagation themselves. Spam can also carry phishing attacks. These are emails which will convincingly appear to be from a legitimate source even when they are not. They will encourage you to enter valuable and sensitive information, such as usernames and passwords and then pass that information on to the wrong people. Thankfully there are many types of anti-spam and anti-virus software available which can limit the risks, even if they can't remove them altogether.

However, one of the largest risks associated with email is very often completely overlooked. When we send information via email, it is open for the whole world to see.

"Many people do not understand that sending an email is about as secure as sending a postcard"

Deborah Hurley, Information Infrastructure Project Head, Harvard University.

What happens when you press send?

When you send an email it will first travel from your computer to your own email server. Almost all IT environments will provide the possibility for this connection to be secure, regardless of whether you are in the office, at home or on the road. The real problem occurs when your email server sends that email to your recipient's email server. To do this, the email must travel across the Internet, which is public territory and out of your control. On this journey across the Internet, your email can be intercepted with considerable ease.

"Intercepting email is easy to do. Anything that passes across the Internet is bouncing around public connection points where people can listen in. There are tools...that will let you hook in and almost deliver it back to you on a plate" *Greg Day, Security Analyst, McAfee.*

What this means is, that if anyone were to "hack" one of these public connection points known as "routers", then they would be able to view all of the Internet traffic passing through it, including your email! There are Internet sites which will auction off hacked routers, generally referred to as black hat exploits, and whoever bids the highest will obtain access to all of the information that passes through them. This person might be involved in organised crime and it would not be difficult for them to set up an automated system which would read the content for anything juicy that they could exploit. If it were interesting enough then they might start attacking your email directly as a result.

The easiest way for a specific email to be intercepted is via a "man-in-the-middle attack". This scenario occurs when you send an email and a hacker pretends to be your recipient's email server. This results in your email server sending the hacker your email! He can then

pretend to be your email server and send it onto the real recipient once he has copied or even altered the email. The most frightening thing about this is that it can be done without sender or recipient being any the wiser!

How can you prevent this from happening?

The only way to protect against this and ensure that the information you send within emails is kept confidential is to encrypt your emails. Encryption is the process of scrambling information in order to make it unreadable. It is performed by using a mathematical algorithm along with an "encryption key". The only way the information can be made readable once more is to decrypt it using the appropriate key. If a hacker intercepts an encrypted email, as long as the encryption used is strong, he won't be able to read it or make any changes because he won't have the necessary key required to decode it. Many regulatory authorities encourage the use of email encryption.

"Do you warn staff about the insecurity of email and make sure that any sensitive information sent electronically is encrypted or sent by other means?" *The Information Commissioner, 2007. The Information Commissioner is the Government official responsible for upholding the data protection act and has the power to fine any organisation that does not comply.*

Who's reading your email?

Besides the danger of third parties obtaining our emails illegally, many people are unaware of those that have legal access to them. With the increasing fear of terrorist activity, the Government has acquired more power to intercept our communications than ever before in the form of the "Regulation of Investigatory Powers Act". "RIPA" gives a whole host of public bodies varying levels of power to access our communications. Even organisations such as the Ambulance Services, The Department for Transport and local Councils include individuals with some powers to snoop on our communications. It has also been reported that Government ministers want to implement plans allowing them to intercept, store and analyse all of our emails as standard without the need for individual case requests.

"Most unencrypted email is vulnerable to unauthorised access and alteration as it passes over the Internet" "Firms are recommended to adopt systems that... automatically encrypt all outgoing email to those offering similar facilities" *The Law Society Email Guidelines 2005.*

If emails are effectively encrypted then they cannot be read without the necessary key, even by the Government. However, Law enforcement agencies can lawfully obtain keys with "the appropriate permission". If you allow a third party to perform your encryption or hold onto your private decryption key then you could still be in the dark over who has access to your emails. If you use an email encryption service that gives you sole control of your private decryption key then, in order to gain access to the information in your emails, these agencies would need to request that key from you – nothing could be accessed without your knowledge.

If the world wants to continue using email as the preferred method of communication; then unless we encrypt, we continue to risk the confidentiality of our own data as well as that of our contacts.