But why not just email it?

By Joss Milner CA

Sniffing has always had negative connotations, when we grew up our parents always told us stop sniffing. Then in the late 20th century sniffing became associated with drugs. Today in 2009 sniffing has again been associated with a new evil - Sniffing of emails. Sniffing is listening (with software) for packets of data of interest, this is also known as web trafficking. When sniffing software sees a packet that fits certain criteria, it copies the packet. Unfortunately as emails are sent though the Internet as plain text they can be very vulnerable to sniffing.

Email is a very efficient way to communicate with clients, but extreme caution should be exercised in sending confidential information via email. Have you ever thought what happens when you click the send button?

Sending the mail
Your email program connects to your Internet service provider's mail server. Like all Internet traffic, your message might be broken into smaller pieces known as packets. These smaller packets can travel more quickly from server to server, and are reassembled when they reach their destination.

Sorting the mail
Just like ordinary mail is sorted first by postal codes, email messages are sorted by domain. The domain identifies where the message needs to go. Each domain name maps to a unique Web address, called an Internet Protocol (IP) address, which is a string of numbers by which each server is identified, the same way a street address identifies a physical location. These relationships are stored in the Domain Name Registry. When the email server receives a message, it looks at the domain and checks the registry to determine what IP address to send the message to. Once it determines the proper destination, the email message is sent on its way.

Delivering the mail
Your message will travel between several transfer points before reaching its final destination. Each transfer point identifies the domain, and passes the message to the next transfer point. This process is repeated — the message getting closer and closer to its destination — until the correct server is reached. Once a message reaches the appropriate domain server, it's channelled into the right email account and stored until the user logs in and checks for mail.

Why is email so unsafe?

- Email messages are sent in clear plain text, making them inherently vulnerable to any cracker who gains access to eave drop and sniff your email.
- Email messages have to go through intermediate computers before reaching their destination, meaning it is easy for others to intercept and read messages.
- Many Internet Service Providers (ISP) store copies of email messages on their mail servers before they are delivered. The backups of these are usually unprotected and can remain for up to several months on their server, despite deletion from the mailbox.

According to the Australian Government Office of the Privacy Commission there are two types of email risk, interception of transmissions and unauthorised intrusion into networks (hacking). Both are invisible and very dangerous.

Surely hackers aren't interested in my clients?

Tax Returns contain sufficient information for an identity theft. A CNN article '*Hackers shift focus to financial gain*' noted that while in the past hacking predominantly targeted large corporations, usually for mere notoriety, these days attackers are seeking financial gain from smaller companies.

What about security through obscurity?

Some security professionals argue that email traffic is protected from a "casual" attack through the vast numbers of emails sent every day making it difficult for an individual cracker to find, much less to exploit, any particular email. Others argue that with the increasing power of personal computers and the increasing sophistication and availability of data-mining software, such protections are at best temporary. Crackers are not looking for particular emails originating or destined for particular people, they are just throwing nets out looking for patterns or themes of information to be used for identify theft/making money.

What should I do about it?

Firstly your firm should not email confidential information such as tax returns, tax file numbers, and the like to clients with at least as a minimum precaution getting clients to sign a confirmation that they understand the risks and are happy for their information to be emailed to them.

Secondly consider using one of the many systems, such as Secure Returns to safely transfer confidential information through the Internet.

Thirdly consider encrypting confidential attachments.

Fourthly if all else fails, there is always good old reliable Australia Post

Joss Milner is CEO of Secure Returns Pty Ltd. A Company that provides secure file upload, download and storage for the accounting profession and their clients.