ViryaTechnologies
ETHICAL TECHNOLOGY SOLUTIONS

Email: Beneficial or Just another Attack Vector?

Email, is it a useful utility or just another attack vector? This article aims to evaluate both the risks and the benefits of using E-mail for everyday tasks.

Many of the risks posed by E-mail are quite obvious to the user, there can be very few users unaware of the risks of 'Phishing', and there forever seems to be news articles about celebrities that have had their E-mail accounts 'hacked'. There are however a number of risks that are not so apparent, E-mails can be intercepted or even 'Spoofed'. In fact in many mail clients it is trivial to make it look like an E-mail has originated from another persons E-mail account, whilst the more Savvy users may check the original headers, many users would not think to do this, let alone know how to view them (In fact the more recent versions of Outlook don't allow you to do so.)

So why would someone 'spoof' an E-mail from you? Aside from Phishing there are many other benefits, I could for example, pretend to be one of your old friends in order to get your home address, or as a prospective employer in order to get your social security number. There are many other uses that such an attack could be used for, the actual likelihood of such an attack is reasonably small as most E-mail attacks are generally sent out 'en masse'.

How many users have signed up to something on the net, only to be asked to re-confirm some security details by E-mail? Did you send the details back? Most people would, but that E-mail could have been intercepted somewhere along the journey, unlike sending details through the post, emails can be read and copied wihtout leaving a trace of evidence. If you are planning to send personal details via E-mail, make sure you encrypt it first. If the recipient doesn't have the means to provide you with an encryption key, ask them if you can provide the details in a different format (Phone, Mail etc.).

How many times have you opened your inbox only to see an email with the subject Fw: Fw: Fw: Fw: Fw: Look at this!!!, Chain Mail is an in-avoidable security risk. You may opt not to forward it on, but it's too late. Your E-mail address has been sent to other people without your consent, if at some point someone receives that chain mail and decides to sell all the addresses to Spammers, your address will be on that list. It increases the likelihood of you receiving spam, Phishing Emails and all manner of rubbish. Sadly, in my experience, asking your friends not to send you chain mail is futile, it just keeps coming through. If you are going to send mail like that, try putting the list of names in the Blind Carbon Copy (BCC:) box, it means that the list of E-mail addresses is private, and protects your contacts.

Other risks presented by E-mail vary, but if your E-mail inbox contains personal information, you should be very aware that this is potentially available to anyone with a mind to access it. Is your password security strong? Does your E-mail provider patch regularly, and do they test those patches before employing them? A security breach may not necessarily be any fault of your own, but the risk remains yours.

If you use 'Webmail', can you be sure that your E-mail is not being read by someone else? A so-called Man-in-the-middle attack is where a system puts itself between your computer and another system, anything you access on the network will pass through this system and potentially be logged and analysed. A good example ofthis attach vector can be found by searching for details of Phorm and BTWebwise on the Internet, although the companies involved claim the system is legal, the methods employed are very similar to those used by black hats.

So those are some of the potential dangers of using E-mails, but surely it does have some benefits? Let's take a look at some of these;

E-mail is (almost) instant, whereas traditional post takes quite some time, E-mail usually arrives within minutes. This can be beneficial when you need a quick response, but a phone call would be far too expensive.

You can ask for a Read-receipt and a Delivery-receipt to verify that the E-mail has indeed been received and read. However this is not guaranteed, systems can be configured to not provide delivery receipts, and most E-mail Clients will allow the User to not sent a Read-Receipt. So whilst the means is there to prove receipt of a communication, there are ways to work around it.

With use of Cryptographic signing you can prove that the email came from you, this reduces the effectiveness of 'Spoofing' and also means that no-one can pretend to be you. However implementing Cryptographic signing does require some End-User training, especially in ensuring that people observe proper security protocols.

E-mail is generally quite convenient but it does have a variety of problems, many companies and courts will not recognise forms or contracts made over E-mail simply because it would be too easy to fake. Users are at risk when using E-mail, especially those who seem to ,inexplicably, lack common sense. Users should be taught not to open unusual e-mails, but in many cases explaining to them that just by opening it they could infect their computer is simply not enough. Many users simply lack the technical knowledge to identify even the most basic risks, and many believe that by placing details in a password protected document they have secured those details.

There is without a doubt an inherent responsibility to hvaing s system connected to any network, and many of the users simply do not measure up, so it is the responsibility of those who do understand to educate them. This article has detailed a few of the risks posed by e-mail (including the wane in correct grammar and spelling), but there are many many more. E-mail is a useful commodity, but it does carry some severe risks if not managed and implemented correctly.

Many users would claim that they could not live without e-mail, but interestingly we recently had an issue with our E-mail server. In evaluating whether to remove E-mail rather than invest time and resources in repairing the system, we reached the conclusion that one user required E-mail. Everyone else could function without it if they needed to, we would have been highly unpopular if we had not decided to repair the system for the sake of the one, but it did highlight how little need there actually is for e-mail.

I hope this article has opened your eyes to some of the risks and benefits of E-mail, the benefits vary between users but it would appear that E-mail is quite often a luxury. It is certainly taken for granted, and a lack of technical knowledge on the subject can often lead to dangerous repercussions.

About the Author

Ben Tasker is an IT Manager & Linux Specialist at Virya Technologies. He has substantial experience within the IT Industry, and a keen interest in Network security.

More whitepapers and free resources available at http://www.viryatechnologies.com/