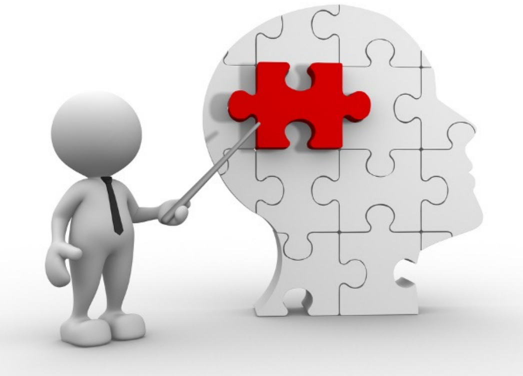
UNDERSTANDING EMAIL



Email is a complex system and most of the time we just see the top 10% - what we get in the inbox. In most cases that is enough! All of that SPAM %}^%{**.

For mail to traverse the digital world there are a number of factors that have to be aligned so that it can be sent from someone to you and back again. It can be complex! Very complex at times.

The email system has been around practically since the inception of the Internet in 1985. Little of it has changed in that time.

We had the introduction of SPAM in the early 2000, it started with Nigerian princes wanting money and people wanting bigger and stronger appendages with Viagra. SPAM came about because email can access millions of people with the same message for no cost to the sender. Started off as more of a nuisance, a bit of a giggle.

Then the criminals got onto it. The cybercriminal saw the benefits of email and now it is the attack weapon of choice. In the last 5 years they have perfected it into one of their delivery systems targeting the uneducated, ill-informed and ignorant.

The criminals created the phishing email, an email designed for you to open up a link, hence the fishing analogy (baited).

Since 2010 we have also had spear phishing email. These are specific emails that have been targeted at the individual person who it is addressed to. The criminals have done research through social engineering and made the email more enticing.

You can now understand that email is not all it's cracked up to be, and all users of email should be aware of the problems that it can deliver to your organisation or your home.

The four rules of email and business security

1. **Do not open attachments** - if you need to open it then move the email into the SPAM folder and open it there (outlook) as this folder will not allow an executable file to execute.
2. **Do not click on links** - this is the same as above, if you think it is important and you were expecting the email hover your mouse over the link and see where the link will take you. If it is URL shortened (bit.ly) then move it into the spam folder and click on it from there. If you do click on a link and it takes you to a website that says you need to install something - see point 4
3. **Do not put confidential information in an email** - Email is a broadcast medium. Anyone can get an email and reply, forward it on or print it.
4. **Use common sense** - the crypto locker virus comes into businesses as an email from either ATO or Australia Post. If you receive these type of emails ask yourself one question - "how did they get my email address and would they email me that information?" If they shouldn't have your email address then it is SPAM.
   The criminals need you to install their malware so if you are ever asked to install Java, adobe or flash. Ask yourself this question, it was working before, why is it not working now. Then cancel the installation process

The reasons why you cannot send or receive email

1. **Recipients SPAM filter too tight** - we have all experienced it, someone telling you they sent you an email and you have not received it. There is a high possibility that the sender is on a black list and your system will not accept email from them because of it. DO NOT ask your IT department to white list that domain as you are opening up your business to attack. Tell the sender that they are on a black list and they need to resolve the problem at their end. (Remove from black list and scanning their systems for malware)
2. **Domain sending out SPAM** and has been black listed - it has to be removed from the black list. Different filters use different black list suppliers. Any one on that supplier will not receive email from domains that have been black listed.
3. **The Internet Nazi's have put you on a black list** - you have done a mass mailing through your mail server. And someone has complained. If you have to do a mass mailing then use a system that is designed to do it!

Every time you get a bounce message for an email that has been returned there is an error code. That error code will tell you explicitly why the email could not be sent to the recipient. My email is bouncing is not an error message. Look at the message and send that error message to your IT support.