OPENING EMAILS SAFELY

One of the most common problems we face when it comes to virus interaction, is someone opening an attachment on an email they believe to be safe. Recently the emails received have gotten more and more convincing. Everything in the email says 'open me, I am important.' But please spend that extra time checking.

IDENTIFY SENDER

When you receive an email from a new contact you can automatically mistake it for a new business associate, open it and any attachments. The first step is to confirm the sender is genuine. You can do this by searching their email online. If the email is fake it will generally show up as such. Also, people tend to use aspects of their business or real name in the email. We have @abm.uk.net at the end of ours.

ATTACHMENTS

With attachments, be careful to check the file type. You do not have to click on it to do this, the icon will generally tell you what the attachment is. If you can't identify what the item is through the image, then there will be an indication in the title. For example, 'File Opening Procedures .docx' Generally .docx and .pdf files are safe, if you are expecting them and know the sender. File types that are strange to see are .exe, .bat and .msi. These are programs and are not usually sent via email. Some dangerous files are saved in containers, for example, .zip or .rar files. If you receive these when you are not expecting them, do not open them. If you really want to check the attachment because everything else mentioned seems trustworthy, there are ways. You will need an anti - virus program installed on your machine. The way we like to do this is: **Right** click on the file and save it into a temporary location. Somewhere away from other files, in an empty folder. From here, go to the location where it is saved. **Right** click again on the file and choose the option to scan it with your anti-virus software. This will only be effective if your software is up to date. It will give you an idea if the file holds anything nasty.

LINKS

If there are not only attachments but links in the email. Check the authenticity of these as well. You can do this by hovering over the link and a URL should appear. DO NOT click on it. Just hover over and see if it looks legitimate and recognisable. If it seems like the URL of a website for the company you are working with then that is a good sign. You can always go to a search engine and search the company to check.

READING THE EMAIL

When receiving an email you are not sure about, the simplest thing to do is to read the content. Have they got your name right? Have they mentioned what you expect? Have they shown abnormal urgency for you to open any attachments? Have they got a professional demeanour within the email? Do they have a signature at the end of the email? But most of all, does the email read right? If this person is doing business with you or vice versa, the email will have some formality and the person should have checked grammar, spelling and punctuation. Also check for other languages in the small print or footer that are unexpected.

It is honestly better to be safe than sorry. Having a virus can cause more affects than you realise. And in some cases, can shut down a whole business. If ever in doubt, pick up the phone and talk with the sender, or reply back and just double check, this way you can confirm if all is genuine. We are happy to assist with prevention and to give some ideas on how to install processes or key information within your business so no harm comes to your systems.