Cybersecurity for Charities

Cybersecurity Briefing

CSB_001 | 01072017 | info@martynandvalerie.com eMail

Introduction

Whilst eMail is probably one of the oldest technologies used for communicating, it still remains the most preferred way to enable us to communicate and share information with our colleagues and friends, whether for business or private purposes. However, like most digital solutions, it increasingly poses a threat to our personal and organisational information security.

Learning Points

Incoming Threats

Attachments continue to be a major threat to our information security. Viruses are commonly spread in this way, causing untold damage to your data, or by simply creating chaos that results in slow performance of your systems.

The latest scourge is Ransomware that can, but not solely, be transmitted via eMail. So you receive an eMail with an attachment and you routinely double click to open the attachment, out of curiosity perhaps? Suddenly, all the files you have permission to access are encrypted, and can only be unencrypted by paying the ransom. Ouch!

Then there are the phishing eMails. Those that purport to be from a bank, or from one of the companies you deal with, such as Apple, asking you to confirm your account details. Some look very convincing, however no respectable bank or supplier would ask for this information by eMail.

And spam, well that's just electronic junk that takes up your time and the time of your organisation in so many ways. By opening a spam eMail you are validating your eMail address giving the spammers another tick on the list.

Make it difficult

Hackers trawl web sites for eMail addresses and collate these into sizeable lists that they can use and abuse. So you could reduce the amount of spam you get by not publicising your actual eMail address on a web site.

You could also adopt the technique of placing your recipients in the Bcc field of your eMail header, rather than in the To field. This reduces spam and the overuse of the Reply to all command!

Remember that eMail is public, unless encrypted, so don't write anything offensive, incriminating or private in your communication unless you can ensure its privacy, which will always be difficult. Once written and sent it would be almost impossible to delete. Think of an eMail as a postcard.

And, most important, always check you have correctly addressed your eMail, especially if you rely on autocomplete features.

Tips

- If you receive an eMail or text asking you to verify your account details – don't reply. Call the provider who is allegedly asking for this information on their publicly known number and verify the request
- Never be tempted to click on a link in a potential phishing eMail
- Never open an attachment if you don't recognise the sender and you are not expecting it. Curb that curiosity
- Delete spam immediately. Don't waste time reading it or forwarding it to others
- Keep your anti-virus up to date and don't switch it off
- Don't write anything in an eMail that you wouldn't want to see out of context
- Never forward eMails without permission

Next Steps

- Check all your eMail for potential spam and phishing and delete them immediately
- Set up a rule in your inbox to filter out all eMail into an advertising mail folder that has the word 'unsubscribe' in the body text.