Manchester Community Central
Supporting our voluntary and community sector
Managed by Macc

CYBER SECURITY...

...it's mentioned everywhere, it's important we all know we should probably do something about it but aren't sure what to do, where to start, whether it will sap our time and energy, detracting from delivering important activities and services.

The National Cyber Security Centre describes cyber security as:

'how individuals and organisations reduce the risk of cyber attack. Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access – both online and at work – from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.'

Breaches in cyber security can lead to personal data being stolen, precious time and money spent rectifying problems, damage to your organisation's reputation meaning people lose trust in you. No one wants that!

How can you stay cyber security safe?
This is definitely a wide area to tackle so if you don't know where to start, try reading our simple top tips below as a gentle introduction. There is so much more to cyber security than this but you might be surprised (and even encouraged) to find that you already have in place some simple cyber security measures, meaning you can start to look at the next steps for your organisation. If not, don't despair! Hopefully this list will provide simple ideas that you can act on more or less straight away and without breaking the bank (or your back) to build a bit of confidence.

Plenty of training is available now and much of it is free; why not take the plunge and find out more by signing up for some now? Find a collation of the sector's training here under 'Digital'

Manchester Community Central
Supporting our voluntary and community sector
Managed by Macc

TOP TIPS

To Improving Cyber Security

Make sure you and your organisation have got the basics covered:

01 Install and turn on up-to-date **Antivirus software** and firewalls on all devices

02 Enable **automatic updating** on your devices, or if this is not possible, regularly update devices manually

03 Review your **privacy and security settings** on your devices, accounts and Social Media pages

04 **Passwords:** Use long passphrases rather than short words, and use numbers and characters, for example: 'FilmPlayTheatre6!' and avoid easy to guess words like 'password1' or birthdays.
Don't use the same password for multiple people or accounts, and never give out your password.

05 Set up **Two Factor Authentication (2FA)** on your accounts - if your password is stolen, the account still can't be accessed

06 **Check links/emails** for legitimacy. If you're unsure, hover your cursor over the link (**but do not click**) until the link destination pops up. Educate your organisation on phishing emails

07 **Log out and lock**: when finished using a device or account, ensure everyone logs out and/or locks it to prevent access to unauthorised users. Make sure devices are **never** left open and unattended.

What should I do next?

Manage user privileges

Consider Security Awareness Training

Backup data