Protecting data whilst volunteering from home – 10 top tips

Tip 1 – Don't share your computer

When possible, use one computer for volunteering and a different computer for everything else. Never let your kids or other family members use the computer you use for volunteering.

Personal computers can have different user logins. If you use a family computer to manage volunteering activities, use a specific login exclusively for volunteering. This ensures your MS Society volunteering files and activities remain separate from your family folders. Use the tools provided to login to your MS Society email. You can find out how to do this along with other useful information here.

Tip 2 – Keep it digital

Avoid printing confidential information onto paper. If you must, make sure you don't leave these documents laying out or unattended.

When you're done with these documents, shred immediately. Never place them in the rubbish or your household recycling.

Tip 3 – Verify unusual or unexpected phone calls

Cybercriminals will often call employees or volunteers pretending to work in the IT department.

If you receive an unexpected call, never give out your password, MFA generated numbers or any private or confidential information.

If you're unsure, stop and call the Volunteer Support Team.

Tip 4 – Update your computer

Make sure your computer is up to date with the latest patches and upgrades when prompted by your system.

When in doubt contact your IT/antivirus provider for help. Computers that don't have the latest updates are easy targets for cybercriminals.

Tip 5 – Beware of phishing scams

When you receive an email, even if it comes from a fellow volunteer, MS Society employee or friend, avoid clicking on a link or opening an attachment unless you have verbal confirmation from the sender on what it is.

Remember, email is the most common way to spread malware. Once malware is on your computer, anything you can access, the criminal can access. This includes websites, email and even the organisational network.

Tip 6 – Beware of malicious text messages

A mobile device can be just as vulnerable as a desktop computer. Beware of malicious apps and never click on links received in unsolicited texts.

Tip 7 – Be cautious with Wi-Fi

Never use unsecured public Wi-Fi for volunteering purposes. The problem with unsecured public Wi-Fi is that you have no way of knowing who controls the access point. This means that a criminal could be monitoring everything you're doing while connected in public places.

Tip 8 – Secure your home Wi-Fi

Make sure your home Wi-Fi has a strong password. A simple password or no password at all, will allow criminals on your network, where they can attack your computer.

Tip 9 – Change that password

Never use the same password more than once. If a website is hacked and a criminal gains access to your password, they will try to use that same password at other sites.

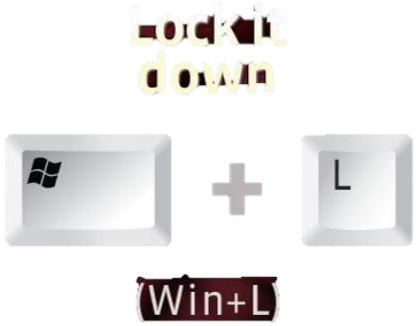
Use a password manager or other system for maintaining unique passwords for every account.

Tip 10 – Lock your computer

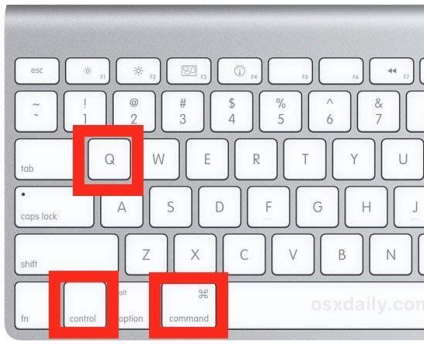
Don’t wait for it to, or assume it will, fall asleep.

When you walk away from your computer, at home or on the go, lock it. It takes one extra second, and it will ensure that you and only you have access to it.

- To lock Windows press “windows key” + L



- To lock Macs press “Control” + “Command” + Q



Additional sources of information

You can find more information on good data protection practices by visiting the volunteer website: https://volunteers.mssociety.org.uk/handling-data.

If you can't find answers to your queries, please contact the Data Governance Team via Volunteer Support or directly at datagovernance@mssociety.org.uk.

Should the worse happen, report it immediately to dataincident@mssociety.org.uk. Copy in volunteersupport@mssociety.co.uk.

Thank you.