Security guidance – your premises – COVID-19

8/4/2020

Below are some basic guidelines for community volunteer groups and VCSE organisations regarding maintaining good security practices - at a time when we are all adapting our ways of working during the current situation with Coronavirus.

These guidelines should be used in conjunction with the advice you've been given by the group or organisation you are working with. These guidelines are relevant to office security but also whilst working remotely.

Security of your premises

Many organisations may have left their usual office/premises unstaffed due to the move across the UK to remote working. Make sure you consider the safety and security of these buildings during this time:

- Keep equipment (such as laptops that might be going to be stored in your office, or cash) locked away securely.
- Check if your locks meet the appropriate British Lock Standard.
- Your usual 'last person out' office policy should be followed - E.g. doors locked, fire doors shut, windows shut, alarms set, electrical items turned off, when possible.
- Train your employees - your security procedures are only effective if your employees know what they are or how to use them. Necessary staff need to be briefed on this as staff may be required to enter the building during this time for urgent work, to pick up post, or perhaps to change the backup disk in the server.
- Ensure CCTV and building alarms are in full working order if you have them.
- Assess data backup needs of your organisation. Is it possible to take back up copies from your server remotely? If not, the necessary staff entering the office need to be fully briefed on leaving the building secure afterwards
- Ensure relevant equipment and materials for remote working are covered by your current insurance policy.
- Lighting outside building entrances has been shown to deter intruders.
- Use a locked post-box if possible. Think about if you are expecting deliveries and how to handle this: can they be diverted to another address?
- If you are using premises to store food supplies these deliveries may need to be left for the recommended amount of time for germs not to be transmitted. Food storage hygiene safety standards need to be followed. E.g. https://www.food.gov.uk/business-guidance/managing-food-safety
- If your staff will all be working remotely, ensure you have cancelled all meetings/visitors that were expected to take place at your office, reschedule these as online meetings. Sign up to Voscur's free online course to help you do this - Running Online Meetings - https://www.voscur.org/calendar/event/running-online-meetings-online-course-0
- If you know your office may still be accessed by the building owners, or cleaners, and you have specific security procedures that need following ensure you have informed these people.

- Join a 'business watch' - many police forces have formed 'business watch' schemes, where property owners can alert police and other organisations about burglaries and other crime.
- Update, if necessary, your organisation's insurance policy and risk register to cover new activities, such as staff working remotely (and the office being left empty).

Security of data

- Secure your Wi-Fi - though it should be a priority to keep your office physically safe, you also need to consider the other ways in which your office may not be so secure. Leaving your Wi-Fi open for anyone to use will not only slow your internet down, but it can enable hackers to steal sensitive information. Make sure you password protect it (office and home Wi-Fi).
- Practice basic online and identity security even when working remotely. If working remotely ensure you still run regular software updates, change default router Wi-Fi password, secure all electronic devices with strong passwords, review privacy settings of social media accounts, don't use the same passwords for social media accounts. Read these useful quick tips and guidance issued by Avon & Somerset Police about making your home cyber safe.
- By mindful of confidentiality and follow GDPR best practice guidelines even when working remotely.
- Lock your Server Room if you are able to do this.
- Lock away any legal documents and sensitive paperwork that may need to remain in the office when staff are working remotely.
- Ensure all usual firewalls, antivirus software and all protection against malware is set up and running whether staff are working in the office or remotely.
- Don't connect to public Wi-Fi Hotspots if possible. Use your mobile phone's hotspot instead or a trusted Wi-Fi network.
- Refer to this advice from the National Cyber Security Centre: https://www.ncsc.gov.uk/files/Charity%20Guide%20v3.pdf