green pepper

Cyber Security Checklist

Introduction

Failure to take cyber security seriously can impact severely on an organisation's reputation and finances. But, for example, using passwords, updating operating systems, and backing-up your data can drastically reduce the risk of falling foul of malicious viruses like ransomeware. For detailed advice please see the National Cyber Security Centre website. In the meantime, this simple checklist guides you through the important steps. Don't forget also that it should apply to privately owned devices if they are used for work purposes.

You will want to be answering "yes" below, wherever possible….

Backing-up data

- ☐ Have you identified all your essential data?
- ☐ Do you make regular backups (daily for absolutely essential data)?
- ☐ Do you store back-ups separately to your main computer (e.g. cloud storage)?
- ☐ Is the place you store your back-ups properly secure (e.g. cloud storage)?

Protecting from malware

- ☐ Is your anti-virus software installed and switched on?
- ☐ Do you prevent staff and/or volunteers from downloading third party apps and software from unknown vendors?
- ☐ Have you set administrator-only permissions for installing new apps and programmes?
- ☐ Do you regularly update your IT equipment (computers, phones, tablets etc.) whenever a new operating system version or patch is published?
- ☐ Do you replace IT equipment that can no longer work with the most recent versions of your software, or when devices are no longer supported by the supplier?
- ☐ Is the operating system's own firewall enabled on all desktop and laptop computers?
- ☐ Do you avoid using USB drives and memory cards tor data transfer between devices, and encrypt them if taken out of the office?

Smartphones and tablets

- ❑ Where possible, are devices protected by 6 figure rather than 4 figure passcodes?
- ❑ Have users switched on fingerprint or face identification?
- ❑ Have devices been set up to enable location tracking, remote access lock and remote erasure of data?
- ❑ Are devices kept up to date with the latest releases of iOS or Android operating systems?
- ❑ Are apps updated regularly whenever a new version is released?
- ❑ Do users avoid connecting to public unsecured Wi-Fi and instead use a 3G or 4G mobile network (e.g. by tethering their tablet or even laptop to their phone's 3G or 4G mobile network)?

Laptops

- ❑ Some laptops are more secure than others. Do you have a policy for laptop use regarding passwords, data encryption, attaching USB drives and connecting to WiFi networks?

Passwords

- ❑ Are all your IT devices (laptops, desktops, phones, tablets, modems, routers etc.) protected by passwords or codes?
- ❑ Have all the manufacturer default passwords been changed?
- ❑ Do you use robust individual passwords for your various local and online individual accounts (ie. not predictable passwords)?
- ❑ Have all staff and volunteers been given action advice on setting secure passwords?
- ❑ Do you use two factor authentication for important accounts?
- ❑ Do you avoid unnecessary regular forced password changes on users (as these can encourage the use of weaker passwords)?
- ❑ Have you considered using password managers to store passwords that can be accessed via a single secure password?
- ❑ Do users store in a secure place any written note they keep of their passwords?

Avoiding phishing attacks

- [ ] Do you advise staff and volunteers on how to spot unusual, suspicious or bogus emails?
- [ ] Do staff and volunteers know what to do if they should receive any such emails?
- [ ] Are you aware of your digital footprint (your website and social media accounts, and what information your staff and volunteers share online about your organisation)?

Networks

- [ ] Is your network protected with appropriate firewalls?
- [ ] Is your network protected from attack (e.g unauthorised access and malicious content)?
- [ ] Are network security measures monitored and tested?

Physical access to IT equipment

- [ ] Is access to the office or location of IT equipment restricted or monitored (e.g signing in of all visitors).
- [ ] Are visitors to your premises properly supervised?
- [ ] Does your organisation's premises have suitable security (deadlocks, alarms etc)?
- [ ] Are old hard drives, USB sticks and other redundant devices properly erased and/or destroyed if appropriate?

Personnel

- [ ] Are all your staff and volunteers properly trained in the appropriate use of IT devices, software applications and relevant policies?
- [ ] Are all your staff and volunteers made aware of cyber security measures and their importance, including its relationship to data protection law?
- [ ] Do your staff and volunteers know how to report a cyber or data breach?
- [ ] Does the organisation know what to do if it believes it has been the subject of cyber fraud and/or a data security breach?