THE SENSIBLE SMALL BUSINESS IT CHECKLIST

Use these tips to better defend your business against cyber threats and productivity-killing computer issues.

☐ 1. UPDATE YOUR OS

Security updates may feel like a hassle, but they're critical keeping your computer secure. **On a Mac** > Open **App Store** > Click **Updates** tab in the top menu. > **Download and Install** all available updates
On a PC > Select the **Start** button > **Settings** > **Update & security** > **Windows Update**, and select **Check for updates**.

☐ 2. PATCH YOUR SOFTWARE

Clicking "remind me later" is tempting, but please try to resist and run your updates.
Keeping third-party apps up to date will **fix security vulnerabilities** and **provide better functionality**. To automate the process check out **"Personal Software Inspector from flexera.com."**

☐ 3. DELETE JUNK AND RUN A MALWARE SCAN

Cleanup at least once a month, this will speed up virus scanning and free up disk space. **On a PC** > Use the built-in **Disk Cleanup utility** or install **CCleaner**. Next, download and Install **Malwarebytes** and run a scan, if it picks up anything remove and reboot the computer. Malwarebytes is also available for Macs.

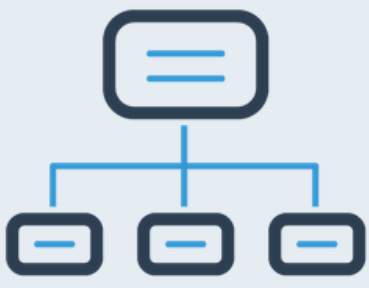
☐ 4. UPGRADE YOUR BROWSER

An outdated web browser makes your computer unsafe.
If you are still using **Internet Explorer**, you need to switch today!
Modern browsers like **Chrome, Safari, Firefox, Edge,** and **Opera** are faster, safer and support a greater range of web technologies.
Don't forget to keep your **browser extension up-to-date** as well.

☐ 5. MANAGE YOUR BACKUPS

Use the 3-2-1 rule, which means you should have (3) copies of your data at all time. Start with a local backup. **On a PC** > Select the **Start button** > **Settings** > **Update & security** > **Backup**.
On a Mac > **System Preferences** > **TimeMachine**.
For a cloud backup solution look into **Carbonite**, **CrashPlan** or **Backblaze**.

☐ 6. UPDATE YOUR ROUTER



Your router/firewall is the most critical part of your network.
Some models update their firmware automatically; most don't.
The update process slightly differs from each model.
You'll find detailed instructions on the **manufacturer website**.
* You may have to **ping your IT guy** for this.

☐ 7. STORE PASSWORDS SECURELY

Passwords must be unique, long, complex and changed regularly.
Protect your important accounts with **two-factor authentication** and prohibit employees from sharing logins with each other. Store your password in a **secure database** like **1Password, Dashlane** or **LastPass**.

**Re-visit the checklist at least once a month*!