

# 5 Ways to Secure Your Small Business Right Now

Use these five steps to make your security better right away - without killing your budget.



STEP	DESCRIPTION
<b>TURN AUTOMATIC UPDATES ON</b>	<p>Most security exploits preventable if you update your system regularly. They are the result of vulnerabilities where patches were available from the vendor long before the exploit emerged. To keep your system up-to-date, turn automatic updates on on your PC. Windows XP comes with the automatic update feature available, you just have to turn it on. Windows 2000 users can download the capability and turn on automatic updates by running Windows Update from the Microsoft web site (<a href="http://www.microsoft.com/windowsupdate">www.microsoft.com/windowsupdate</a>). Download the latest Windows update software and that will give you the automatic option. Auto updates are also available for many of your security products and other applications like your AV software. Turn on the automatic updates for these too.</p>
<b>ENCRYPT YOUR DATA</b>	<p>Encryption is not just for laptops. Wherever you store confidential data - be it yours or your clients' - you should be using encryption. Servers, desktops, laptops, and especially removable media (like USB key fobs and external hard drives) should all be encrypted. Many good encryption tools are absolutely free. Maverick recommends TrueCrypt encryption software. It is easy-to-use and totally free. (<a href="http://www.truecrypt.org">www.truecrypt.org</a>)</p>
<b>SEEK FREE/CHEAP ALTERNATIVES TO EXPENSIVE AND PAINFUL SECURITY TOOLS</b>	<p>Security does not have to be overly difficult - or expensive. There are many free security tools and alternatives to expensive products and vendor solutions. If you want to put an Intrusion Detection System (IDS) into your environment but don't want to shell out thousands of dollars for a vendor tool, try using Snort. Snort is a free IDS that works great and only costs some time and an old PC system to get up and running. (<a href="http://www.snort.org">www.snort.org</a>). For anti-virus, try the free (and highly-effective) AVG Anti-Virus product (<a href="http://www.grisoft.com">www.grisoft.com</a>). There are also great free firewalls and anti-spyware programs out there. You don't have to pay a fortune for good security tools. Check out <a href="http://www.thefreecountry.com">www.thefreecountry.com</a> for a list of great free security tools you can start using today.</p>
<b>SHRED, WIPE, AND OVERWRITE</b>	<p>On PCs, in your dumpster outside, and even inside your copier/printer, the confidential information of you and your clients is accessible to others. Dispose of your data wisely. In the digital world that means three things: shred it, wipe it, or overwrite it. Shred <b>anything</b> with a name, address, or account on it - with a quality cross-cut shredder. Then you can feel free to recycle it. Wipe <b>all</b> digital media you plan to surplus. This means overwriting the media a minimum of seven times. Deleting files is not enough. For media you want to reuse, overwrite it <b>completely</b> prior to reusing it - again, at least seven times. Try free utilities like SDelete (<a href="http://www.microsoft.com/technet/sysinternals/FileAndDisk/SDelete.mspx">http://www.microsoft.com/technet/sysinternals/FileAndDisk/SDelete.mspx</a>).</p>
<b>BACKUP &amp; STORE OFF-SITE</b>	<p>Do you backup your critical data? How often? Critical data includes all customer data, but also any information about your own environment you cannot afford to be lost. These include things like contact databases, Business Continuity/Disaster Recovery Plans, and HR information. Numerous backup solutions exist, both free and fee-based, and should be chosen based upon how big your business is, how much data there is to backup/store, and what level of effort is required to do so. You might consider a provider like Iron Mountain for backups. No matter what your backup solution, your backup data should be stored off-site (not at the location you backed it up at). This can either be done by a provider or by you. A very small business may store backup data in a bank lock box where they keep their accounts.</p>