This free informational report is compliments of Computer Troubleshooters.

Computer Troubleshooters, a worldwide network of computer service franchises, works to meet the technical needs of small business and residential computer users. **We're the computer experts**…the people to call when your computer breaks down, when your machine or software needs upgrading, when viruses attack and even for service plans that guarantee no downtime.

Computer Troubleshooters technicians offer **unique, economical computer solutions and services** geared toward your needs—focusing on products and solutions most beneficial to small business clients and residential computer users. Our technicians combine friendly, personal service from a locally-owned and operated Troubleshooter with the knowledge, support and reliability of the world's largest computer service franchise.

www.computertroubleshooters.com

The Top 10 Technology Mistakes Small Businesses Make

(And How To Avoid Them)

Small businesses typically focus on researching, understanding and managing elements related to their businesses. That's good business sense, after all.

Accountants, in other words, invest time maintaining pace with changes (legislative, economic, etc.) that impact their customers, servicing clients and building their businesses. Physicians, dentists, plumbers, financial services companies, non-profit organizations, automotive dealerships and numerous other small business do just the same.

Few, if any, have time to monitor the daily changes that impact information technology. Even fewer possess the resources necessary to keep current with changes to Microsoft Windows, Microsoft Office, proprietary business software, critical business applications, printing technologies, web-based tools, email services and a myriad of other technology concerns.

Fortunately, small businesses don't need to be experts at both their business operations and information technology. Computer Troubleshooters can help. Each Computer Troubleshooters franchise is independently owned and operated, meaning there's a Computer Troubleshooters technician near you who can act as a valued member of your team.

As you assess your business' software, hardware and networking needs and requirements, we hope you find this report on the top 10 technology mistakes small businesses make (and tips for avoiding them) a useful tool for gauging your business' technology infrastructure.

Typical small business technology support comes from one of several sources:

Mistake #1:

Weak Tech Support

- ☑ One "quasi-support" staff person may be tasked with "looking at" other users' PCs when problems arise. These duties are typically added to the staffer's regular responsibilities, which means critical IT needs are automatically relegated to secondary status. While so-called power users often serve as a wonderful first line of support, they possess their own work duties that, if interrupted, delay other business functions when the individual must put on their "support hat."
- ☑ Telephone support from often-distant PC and software manufacturers, which often covers only limited issues, is of poor quality or fails to appropriately address an organization's business objectives.
- ☑ "Unprofessional" IT consultants (or computer technicians who provide service "on-the-side") who may not show up when promised, may charge too much for service and who may frequently prove "stumped" by more difficult computer problems, network issues or proprietary application troubles.
- ☑ Big-box electronic stores whose technicians: may be learning the information technology trade and may not possess the experience of a full-time consultant, likely suffer frequent turnover (meaning it's less likely you'll receive the same technician twice and therefore must start from scratch each time your business experiences an issue) and may be more motivated to sell unnecessary equipment or upgrades.

Small businesses can avoid and overcome these issues by developing a service relationship with a qualified information technology partner. Professional, dedicated technology consultants:

- ❖ Resolve problems faster
- ❖ Possess significant computer and network knowledge
- ❖ Grow in ability to better-server your organization the more they work with you
- ❖ Help minimize disruptions
- ❖ Fulfill specific technology needs
- ❖ Complement existing "quasi-support" staff
- ❖ Deliver cost-effective, proven solutions

Computer Troubleshooters, the world's largest computer service franchise with 470 owners and operators worldwide, serves just such a role for numerous small businesses. Its technicians, as well as those from other respected consultancies, can provide assistance in a wide range of areas, including: hardware and software troubleshooting, Internet/email setup and maintenance, networking and Internet security, application setup and support, regular computer maintenance and service plans, Website design, virus and spyware protection and removal, remote assistance and more.

Accountants typically amortize computers after three or four years. There's a good reason for that: older computer systems usually cost more due to lost efficiencies, compatibility issues, service and maintenance and downtime.

Mistake #2: Old, Cheap or Inconsistent Hardware

Developing a solid hardware replacement plan can help ensure your organization maximizes its IT investment. Darin Stahl, a lead analyst with Info-Tech Research Group, said in a January 2008 article that "when you look at costs—particularly around a four- to six-year lifecycle—it may seem like you are saving money, but really it's costing you, because you are going to increase your support costs."

Instead of encouraging failures and downtime, Computer Troubleshooters can work hand-in-hand with your business to develop a hardware lifecycle plan that makes sense, thereby ensuring you avoid the following common Old, Cheap or Inconsistent Hardware Issues:

- ☑ Old hardware that is much more likely to experience frequent problems, failures and downtime and that prove more difficult for technicians to properly service.
- ☑ Cheap hardware that is more likely to experience frequent problems and compatibility issues and that, like old hardware, prove more difficult for technicians to properly service.
- ☑ Inconsistent hardware (such as when each staff member is using a different model PC with different hardware components and software applications) slows technicians when diagnosing problems and increases maintenance costs.

Working with a reputable technology partner to replace computers regularly helps ensure your organization deploys consistent, high-quality hardware, standardizes software applications and maximizes technology investments.

Power protection is another element that often receives little attention but can make a very big difference.

Mistake #3: Inadequate Power Protection

- ☑ Small but consistent power surges (spikes) and drops (known as brownouts) dramatically reduce any technology device's lifespan. This is especially true for computers, printers and other peripherals. Worse, small but consistent power surges and brownouts affect most every business.
- ☑ Surge suppressors vary widely in quality.
- ☑ Surge suppressors wear out over time (and often without indication).
- ☑ Common power strips provide no electronic surge or lightning strike protection.

Computer Troubleshooters technicians can work with you to determine how your equipment and network should best be protected from electrical surges, brownouts and even lightning strikes. Typically solutions involve:

- ❖ Deploying high-quality surge suppressors for all computer equipment, printers, fax machines and other peripherals.
- ❖ Replacing surge suppressors every two to three years.
- ❖ Identifying locations where uninterruptible power supplies (UPS) with line conditioning are a better match for protecting critical network equipment and computers.

Several simple steps help protect PCs, network equipment and data from damage and loss. While no method is foolproof, **Computer Troubleshooters recommends** small-business owners follow these three strategies to minimize electrical threats:

1. *Use only high-quality, brand-name surge protectors and battery backups*
2. *Insist on network protection.*
3. *Connect equipment properly.*

Software licensing issues can prove perplexing. OEM licenses, often purchased with new computers, cannot legally be moved to another PC. This is true for many copies of Microsoft Office and Microsoft Windows. Other applications, such as free versions of many popular antivirus and antispyware programs, and Microsoft Office Student & Teacher Edition cannot be legally installed in any business.

Mistake #4: Illegal Software

It's estimated that software piracy costs the industry more than $11 billion annually. As a result, software vendors are very aggressive in pursuing small businesses that deploy and use improperly and illegally licensed software.

Technology partners such as Computer Troubleshooters can help protect businesses from disruptive investigations, the use of illegal software and resulting fines. With a professional technology consultant's assistance, small businesses can receive expert help ensuring they properly license software for each and every PC, remain protected from audits with proper documentation and avoid the following common failures:

- ☑ Many businesses don't realize that they do not "own" software. Instead, businesses typically own a license to use that software on a specific number of PCs.
- ☑ Some businesses use "borrowed" software obtained from an employee's home computer or friend.
- ☑ Many software programs report their usage back to the manufacturer via the Internet. Microsoft and Intuit (Quicken, QuickBooks, etc.) products especially report their use and require activation to continue working properly. The receipt of audit notifications or breach-of-license letters is becoming an increasingly common occurrence as a result.
- ☑ Murphy's Law plays a role; unlicensed or under-licensed software usually causes problems at the worst possible time, and they usually compound problems when a technician is attempting to rebuild a mission-critical PC.

The Business Software Alliance reports that 22% of software in North America is unlicensed.

Computer Troubleshooters recommends taking these steps to combat illegal software:

- ❖ Purchase software only from reputable technology partners
- ❖ Store product keys, certificates of authenticity, licenses and original installation media in a single, easily accessible location
- ❖ Read license agreements carefully when installing software and ensure your organization's intended use meets the publisher's requirements

Training is a significant issue for small businesses. This is particularly true for organizations that don't possess their own training department and those that struggle to maximize software programs, applications and technology capabilities or even determine what tools are available to help their offices work more efficiently.

Mistake #5: Inadequate Training

- ☑ It is estimated that most office workers understand less than 20% of the available features in the software packages they use.
- ☑ Inefficiencies often result, as processes and tasks that could be completed in seconds automatically if users understood the features are performed manually instead.

Computer Troubleshooters can assist organizations in teaching staff the skills they require to ensure office personnel maximize existing technology investments. Often, training commitments prove a much better "upgrade" for businesses than a faster PC or more memory.

Here's but one example from the real world.

A Computer Troubleshooters office helped maintain high-powered computers for 12 highly talented engineers. The engineering firm employed a single administrative assistant who prepared all the organization's quotes, proposals and estimates. Once, when this admin was on vacation, the Computer Troubleshooters' technician was called to assist in locating a critical proposal spreadsheet. The admin had prepared the proposal a few weeks earlier, but no one could find the file on the admin's PC and it was urgently needed.

Ultimately, it was discovered the administrative assistant only maintained one "proposal" spreadsheet. Each time a new proposal was needed the admin just typed over the single file with new information (thereby losing any record of previous proposals). Further, the admin didn't know how to perform calculations inside a spreadsheet, so all sums and totals were completed manually using a hand calculator.

Like too many small business employees, this staff member was entirely self-taught, so while she knew how to function in her job, her limited skill set meant she was working harder than she should have in order to product results that were less than they should be.

With today's competitive pressures and increased threats from malicious software, security is of paramount concern. But most small businesses are unfamiliar with the steps they need to implement to not only properly protect their systems but to also protect critical data.

Mistake #6:

Weak Security

Thousands of hackers have written malicious programs that regularly attempt to access your computer. They seek, 24 hours a day, 365-days a year, to:

- ☑ Steal and/or delete your business data.
- ☑ Steal and/or delete personal, confidential or proprietary information.
- ☑ Corrupt your PCs and render them inoperable.
- ☑ Compromise your computer's security and turn it into a zombie system that launches attacks on other computers.
- ☑ Without your knowledge compromise your system and turn your PC into a robotic system that sends tens of thousands of unsolicited email messages a day.

New Windows vulnerabilities are identified almost weekly. The same is true with other software products and hardware devices. Without up-to-date security applications, firmware updates, operating system patches and other updates, your small business is vulnerable to attack.

Computer Troubleshooters can assist your organization in locking down its network, securing its systems and hardening every aspect of its technology operations. Typically, Computer Troubleshooters recommends small businesses adopt all of the following security best practices:

- ❖ Use strong passwords on all systems and software.
- ❖ Update Windows systems with the latest security patches and hotfixes after professional testing proves the updates reliable and appropriate.
- ❖ Update applications and software programs with the latest patches and hotfixes as they become available.
- ❖ Deploy trusted hardware-based firewalls and confirm they are properly configured.
- ❖ Secure all wireless networks by leveraging the latest encryption technologies.
- ❖ Install and configure reputable antivirus and antispyware applications and confirm they regularly update and scan systems for infections; do not permit antivirus and antispyware applications to expire.
- ❖ Prohibit the use of such peer-to-peer file-sharing programs as Kazaa, LimeWire and BearShare.
- ❖ Prohibit staff from visiting MySpace and other Web sites known to encourage virus and spyware infections.

- ❖ Discourage employees from clicking or opening any attachments received within email messages.

No small business is immune from the need for reliable data backups. Every small business wrestles with the issue of data backups. Most every organization recognizes the need—sometimes mandated by law—to archive and secure important business data. However, confusion quickly arises in the details.

Mistake #7: Insufficient Data Backups

How should organizations back up their data? What data should be backed up? How often should archive sets be created? How should backups be moved off site?

Computer Troubleshooters can work with your organization to design and implement a backup solution tailor-made to meet its business requirements. Without an appropriate backup solution, disruptions could prove costly.

- ☑ There is a 50% chance an organization will go out of business immediately when critical data is lost.
- ☑ Odds of business failure increase to 90% within two years when businesses lose critical data.
- ☑ On average, data loss costs 19 days of productivity, according to the ICSA.
- ☑ Recovering data from damaged disks is exponentially more expensive than ensuring you possess adequate backups, not to mention much more time consuming.

Common sources of data loss include:

- *Hard disk crashes*
- *Viruses*
- *Hackers*
- *Data corruption*
- *Fire*
- *Flood*
- *Natural disasters*
- *Disgruntled employees*
- *Theft*
- *Human error*

For better backups and data protection, Computer Troubleshooters recommends:

- ❖ Reviewing what information (specific files and folders) is critical to your business and developing a plan to ensure that data is regularly backed up and stored or rotated off site.
- ❖ Determining how much time can safely pass between backup routines within your organization.
- ❖ Testing backup sets regularly to confirm they are working properly.
- ❖ Updating backup routines whenever required by software application updates and upgrades.
- ❖ Automating off-site storage.

- Confirming a backup solution creates secure backups that protect critical data from falling into the wrong hands.

Viruses pose a significant problem for small businesses. In the most basic sense, computer viruses are malicious programs that almost always infect a system without the user's permission or knowledge. Once installed, virus programs work to replicate themselves, transfer information from an infected PC to a hacker's system, distribute very large volumes of unsolicited email, compromise the PC's performance, delete data and even render a system unusable.

Mistake #8: Virus Vulnerability

To spread or complete its mission, a virus requires a host. That's where small business PCs enters the picture: PCs unprotected by firewalls and proper security software can quickly fall prey to infection. Industry statistics demonstrate that PCs connected to the Internet possess a very high likelihood of being affected, and quickly. I recent BBC report demonstrated a Windows XP machine becoming infected within eight seconds (eight seconds!) of being connected to the Internet. According to another report published by the Guardian, "an unprotected computer connected to the Internet for the first time has a 90% chance of becoming infected with a virus within 40 minutes."

Common virus outcomes:

- *Slow PC performance*
- *Lost data*
- *Corrupted Windows installations*
- *PCs are turned into "zombies"*
- *Network interruptions or outages*

Computer Troubleshooters recommends small businesses install and properly configure antivirus software on every PC and server, especially since the costs of recovering systems and data far exceeds the expense of protecting them. In addition, Computer Troubleshooters recommends the following steps for combating viruses:

- Install an effective antivirus program and keep it updated.
- Perform regular antivirus scans.
- Do not allow antivirus licenses to expire.
- Avoid forms of free security software.
- Disable preview panes within email applications.
- Prohibit the use of file-sharing programs.
- Avoid Web sites known to encourage virus infections.

Spyware programs pose as big a risk to small businesses as viruses. Whereas viruses work to replicate themselves, distribute unwanted email, attack other systems or even render PCs inoperable, spyware typically intercepts user information and relays it to third parties and often redirects user commands. For example, spyware can monitor personal or confidential information a user enters and send it to a hacker or prompt so many pop-up advertisements to display that a system essentially becomes unusable.

Mistake #9:

Spyware Threats

Like viruses, spyware usually installs without the user's knowledge.

Computer Troubleshooters recommends small businesses install and properly configure antispyware applications on every PC, especially since the costs of recovering spyware-infected systems (just as with virus-plagued PCs) data far surpasses the cost associated with preventing infection.

In addition, just as with viruses, Computer Troubleshooters recommends the following steps for combating spyware:

- Install a reputable antispyware program and keep it updated.
- Perform regular antispyware scans.
- Do not allow antispyware licenses to expire.
- Avoid forms of free security software.
- Avoid clicking links within pop-up advertisements and unsolicited email messages.

In fact, spyware infestation is so prominent (some estimates place infected PCs as high as 80%) that, depending upon the conditions in which a PC is used, it may be appropriate to operate two different antispyware programs simultaneously.

Common spyware symptoms include:

- *Slow PC performance*
- *Consistent pop-up ads*
- *Redirected (hijacked) Web browsing sessions*
- *Internet connectivity issues*

The previously mentioned nine issues are certainly sufficient to prompt technology-related headaches. But the top 10 mistakes small businesses make don't end there.

Unsolicited email so plagues many small businesses that many organizations are second-guessing the wisdom of ever using the electronic communications medium. Yet, email has become a critical business tool within most companies. Unfortunately, it's commonly estimated that unsolicited mass commercial email messages account for as many as 14 million messages per day, or almost half of all email.

Mistake #10: Spam Habits

Radicatti Research Group Inc. further estimates that spam costs businesses $20.5 billion annually in technical expense and decreased productivity. Fortunately, spam is one of the easier issues small businesses can protect themselves against.

The United States Federal Trade Commission recommends several steps reducing or avoiding spam:

- Do not display your email address in public (such as on a Web site).
- Avoid responding to or forwarding electronic chain letter email messages.
- Greet money-making opportunities (especially work-at-home schemes) that arrive via electronic mail with great skepticism; Be wary of weight-loss program and product advertisements that arrive in email; Ignore credit repair offers received in email; Avoid advance fee loan scams promoted in email.
- Use a reputable email filter.
- Leverage unique (not easily guessed) email addresses.
- Review Web sites' privacy policies before providing your email address.
- Read and ensure you understand Web forms before submitting personal information.

Spam Facts:

- *Approximately half of all email messages are spam*
- *Spam hurts productivity*
- *Spam filters are effective in minimizing unsolicited email disruptions*
- *Spam presents business liability issues (much spam is adult-oriented)*

Computer Troubleshooters can assist your business in minimizing spam's impact. Contact your local Computer Troubleshooters office for more information.