Management Article February 2009
Virus on Your Computer? Yes, It Can Happen.

Week after week, one of my clients or friends loses their computer to a virus. They end up spending hours or days trying to get back to a state of normalcy. Fortunately, I have never lost a PC to a virus, but to make sure that you don't, you must:

- **Have good virus detection software:** I use Norton, but McAfee is just as good. There are a lot of "free" anti-virus programs out there, but saving a few dollars won't mean much if you lose vital data computer. Make certain you have set the software to scan frequently.

- **Have a good software firewall to protect your network**: Again I use Norton, but several good ones are available.

- **Set your virus program to check for and install updates automatically**: Keeping your virus definitions current helps your anti-virus software protect you from the latest threats.

- **Update Your Operating System and other software**: Make certain that you have set your PC to check for updates to the operating system you are using and for updates to the other software packages you use. Many software updates fix critical security vulnerabilities.

Many PC users forget to renew their virus software and firewall protection, or fail to set their PCs so that they update virus definitions, install security fixes to the operating system, and keep other software current.

Anti-virus software packages are resource hogs and can slow the speed of an older machine (older than about 3 years), so it may be time for new machine if you are choosing between performance and protection.

No matter how good your virus protection is, you should be on guard against spoof e-mails. No one is fooled by a request from the Nigerian royal family to help get 100 million out of the country, but more sophisticated scammers can send e-mails that appear to be from reputable companies. PayPal sent out an excellent list of tips for detecting spoof e-mails.

10 ways to recognize fake (spoof) emails

1. **Generic greetings:** Many spoof emails begin with a general greeting, such as: "Dear PayPal member." If you do not see your first and last name, be suspicious and do not click on any links or button.
2. **A fake sender's address:** A spoof email may include a forged email address in the "From" field. This field is easily altered.
3. **A false sense of urgency**: Many spoof emails try to deceive you with the threat that your account is in jeopardy if you don't update it ASAP. They may also state that an unauthorized transaction has recently occurred on your account, or claim PayPal is updating its accounts and needs information fast.

4. **Fake links**: Always check where a link is going before you click. Move your mouse over it and look at the URL in your browser or email status bar. A fraudulent link is dangerous. If you click on one, it could:
    - Direct you to a spoof website that tries to collect your personal data.
    - Install spyware on your system. Spyware is an application that can enable a hacker to monitor your actions and steal any passwords or credit card numbers you type online.
    - Cause you to download a virus that could disable your computer.
5. **Emails that appear to be websites:** Some emails will look like a website in order to get you to enter personal information. PayPal never asks for personal information in an email.
6. **Deceptive URLs**: Only enter your PayPal password on PayPal pages. These begin with https://www.paypal.com/
    - If you see an @ sign in the middle of a URL, there's a good chance this is a spoof. Legitimate companies use a domain name (e.g. https://www.company.com).
    - Even if a URL contains the word "PayPal," it may not be a PayPal site. Examples of deceptive URLs include: www.paypalsecure.com, www.paypa1.com, www.secure-paypal.com, and www.paypalnet.com.
    - Always log in to PayPal by opening a new web browser and typing in the following: https://www.paypal.com/
    - Never log in to PayPal from a link in an email
7. **Misspellings and bad grammar:** Spoof emails often contain misspellings, incorrect grammar, missing words, and gaps in logic. Mistakes also help fraudsters avoid Spam filters.
8. **Unsafe sites:** The term "https" should always precede any website address where you enter personal information. The "s" stands for secure. If you don't see "https," you're not in a secure web session, and you should not enter data.
9. **Pop-up boxes:** PayPal will never use a pop-up box in an email as pop-ups are not secure.
10. **Attachments:** Like fake links, attachments are frequently used in spoof emails and are dangerous. Never click on an attachment. It could cause you to download spyware or a virus. PayPal will never email you an attachment or a software update to install on your computer.

Don’t forget to go the website for my new book, www.greenweenies.com, to learn all the backroom business terms. There are 1,200+ terms in over 300 pages, with hilarious illustrations by world famous Gahan Wilson. You can register there for your free weekly “green weenie.” If you want to know what a three fingered booger is, or what’s in a train wreck envelope, it’s the only place to go!

Remember, only you can make BUSINESS GREAT!

Please e-mail if you would like me to send previous articles.

AutoSalvageconsultant.com was formed in 2001 to help recyclers improve their businesses. With over fifty years of experience in three staff members, the group is THE definitive source for recyclers’ management and training needs. The founder, Ron Sturgeon, is past owner of AAA Small Car World. You can review his resume, with skills and experience, at our website. In 2002, his book *How to Salvage Millions From Your Small Business* was published to help small business owners achieve significant success. It was recently reprinted in the U.S. and published in China, Korea and the Czech Republic. You can learn more about how to help your business at **www.autosalvageconsultant.com**. You can reach us at 5940 Eden, Haltom City, TX 76117, or by calling or e-mailing Mike Gibson or

Tammy Sturgeon. Mike can be reached at 817-925-0061 or mikeg@autosalvageconsultant.com, and Tammy can be reached at 817-999-1224 or tammysturgeon@all-import.com.