

**JANIS WEBER**  
**"THE MOUSE TRAP"**  
**Sylvania Advantage, Sylvania, OH**  
**August 1, 2011**  
**jwpctutor@gmail.com**  
**419-318-9112**

### **PROTECTING A WIRELESS PRINTER:**

You don't really need to secure your wireless printer. Rather, you need to secure your wireless router. This will protect everything connected to it. Your router is the hub of your network. That's what hackers will attack. Your printer wouldn't even be viewable unless a hacker was already on your network. You may also be able to print over the Internet. This is a cool feature of some newer HP printers. HP ePrint is a seamless way to access your home printer anywhere. And it's as easy as sending an email. Your printer is assigned a random email address. Then, you email your printer what you want to print. The printer routinely checks that email address. The printer automatically prints anything in the inbox. Then, of course, you end up with a physical copy of whatever you emailed. Security of the printer in this respect is entirely dependent on that email address. You want to think of that email address as a password. Do not give out the address. You certainly don't want your printer to start churning out spam messages! Anyone who has that email address can print to your printer. Fortunately, HP does give you one extra security feature. Register your printer with HP online. Once you've done that, you can limit access to the printer. You can specify up to 500 email addresses. Any print jobs sent from other email addresses are ignored.

### **REMOVING AN 'INDESTRUCTIBLE' VIRUS:**

TDL-4 has been described as "indestructible." There are a few different reasons for this. First, it is a rootkit. This type of malware is extremely difficult to detect. It can hide on a machine without the owner's knowledge. Many security programs can't detect rootkits. Second, the TDL-4 rootkit gives the criminals total control over your machine. They can use it to launch attacks. They can install malicious programs. If the server that controls TDL-4 is shut down, it uses peer-to-peer technology to get new commands. TDL-4 has been called the most sophisticated malware to date. Fortunately, though, it isn't really indestructible. If you haven't updated your computer in a while, this could be the problem. Microsoft released a fix using the Microsoft Security Removal Tool. Updating Windows should take care of TDL-3. Viruses are nothing to laugh at. Hackers are constantly finding ways to make them more dangerous. Plus, there are over a million of them out there. At some point, your computer will become infected. If you're lucky, your security software will be able to remove the virus. However, some viruses can disable security software. They can also prevent you from installing new security software. When that happens, you need a more powerful solution. You could try the latest security tool from Microsoft. It's called Standalone System Sweeper and it's based on Microsoft's Security Essentials. System Sweeper works a bit differently than regular security software, however. You don't install it on the infected computer. Instead, you use it to make a bootable CD. The CD lets you boot the infected machine with a recovery operating system. This keeps the virus from activating during startup. The virus can't protect itself, which makes it easier to remove. There are two versions of System Sweeper you can download. One is for 32-bit Windows systems. The other is for 64-bit systems. You want to download the version that matches the infected computer. For example, if the infected computer is Windows 7 64-bit, get the 64-bit version. The System Sweeper disc doesn't have to be created using the infected computer. You can create the disc with any Windows machine. It can then be used on the infected system. This is helpful if the infected machine is completely unusable. Once you select a System Sweeper version, download it and run it. A wizard will walk you through the steps of creating a boot disc. You can use a CD or DVD. Once you select the media type, System Sweeper will do the rest. Once the boot disc is created, it's just a matter of using it. In most cases, this shouldn't be difficult. Put the disc in the infected computer and then restart the system. Some computers will be configured to boot from removable media first. In that case, System Sweeper should start automatically. Be sure and set your infected computer to boot from CD or it will not run.