

When Viruses Attack

Living in a rural area doesn't give you immunity against computer viruses, but take these precautions to protect yourself. **BY CLAIRE VATH**

While working on my computer one weekend an instant message from a friend popped up on the screen with a link to some photos. Intrigued, I clicked the link. Nothing happened.

I clicked again. Nothing. Determined to open them, I copied the link into the body of an e-mail, sent it to myself, and moved over to my husband's computer. When I called up the e-mail I'd sent myself, I clicked the link. Voilà, it opened like a charm. And that's when things went horribly wrong. My husband's computer immediately became infected with a particularly aggressive virus.

But rural computer expert and technology columnist John Deans says that situations like mine aren't uncommon. "Even in rural areas, local hackers and bad guys from the other side of the world will find and hack any unsecured computer system," says the Brenham, Texas, author of "Start & Run a Rural Computer Consulting Business."

While no computer is immune, PCs are more susceptible to viruses over Macintosh computers simply because those programming the viruses write them for PCs, which are more widely used.

The most common threat to the average computer user is malware, Deans says. "This includes spyware, Trojans, rootkits and viruses." And if you're wondering, the term malware is just as daunting as it sounds: It's short for malicious software.

So how do you know if your computer is infected? Mine made it blatantly obvious—frozen applications and frequent crashing—but you won't necessarily get a picture of a bomb on your screen. Some viruses replicate themselves until they fill up your hard drive; others simply may slow down your computer. Your computer may crash repeatedly in the middle of an operation. Files or applications may not run as a result of corruption, and programs may have a strange appearance.

Fortunately, a little prevention goes a long way. Make sure your computer has good antivirus software installed. If your virus scan is up to date, it automatically should detect and notify you that an abnormality has been found on your system. Deans recommends AVG AntiVirus from www.avg.com.



There are a number of other programs that will do the trick, including Norton and McAfee. Spyware is a type of malware that collects information about users without their knowledge. While antivirus software should provide some measure of control for spyware, Deans also advises installing SpyBot for an extra degree of protection (www.safer-networking.org).

Other safeguards:

- ▶ Stay away from obscene or gambling web sites since malware infests the majority of those sites.
- ▶ Make sure, if you have a router for your Internet, that it includes a Firewall, which adds another layer of protection. Read the manufacturer's instructions to determine whether or not you have a Firewall.
- ▶ If you have wireless Internet, make sure there's a wireless encryption of WPA, or at least WEP. Both provide a strong wireless data encryption, protecting outsiders from accessing your connection.
- ▶ Change all default passwords on routers. To increase the security of a password, try a combination of letters and numbers.
- ▶ Use a strong Web browser like Firefox, Google Chrome or Internet Explorer, and keep them current.
- ▶ Allow your operating system to install all system updates, patches and security packs automatically.
- ▶ If a virus has infected your computer, take action. I swallowed my pride and called my husband, who, fortunately for me, happens to be a computer expert. But the best thing to do, says Deans, is "take the advice of your antivirus software." That involves usually one of three things, which your antivirus program will walk you through: heal, move to vault or delete/remove.

Once one or all of those steps has been taken, rerun the scans on all hard drives until it runs clean again. ●