CITADEL
INFORMATION GROUP, INC.

Protecting Your Computer: An Example of Defense-in-Depth.

A reader asks: “What is the possibility of my personal computer being affected? I have two virus protection programs on the computer.”

Dear Reader:

The possibility of your personal computer being affected is high.

Having an anti-virus program (or even two) on your computer is a cyber security requirement just like having a lock on your front-door is required to protect your house and your family.

But if you want to protect your house and family, you need more than a lock or two on your front door. You want locks on all your doors and all your windows, you may want bars on first-floor windows, perhaps an alarm system, maybe a surveillance system, maybe even a 24 hour guard service. If all you have is a lock or two on your front door, there is a high possibility that your house has been robbed.

It’s the same with cyber security. Your anti-virus software — like a spam filter or a firewall — is designed to keep malicious software (malware) from getting onto your computer, just like the lock on your front door is designed to keep criminals out.

Anti-virus software — like that lock on the front door — doesn’t offer very much protection against today’s breed of cybercriminals and the advanced tools they use, tools that virus protection software can’t cope with.

While anti-virus and anti-malware programs may keep the majority of attacks off of your computer, they allow too many attacks to slip through, becoming like invisible ghosts marauding through the house.

That’s why it’s so important to have more than one layer of defense. By itself, anti-virus programs are grossly inadequate to the task of protecting our computers. What is needed is called *Defense-in-Depth*.

The following eight recommendations for keeping cybercriminals off your computer are from our Personal Guide to Staying Safe Online. They are all FREE except for the anti-virus software which you already have.

1. **Keep Systems Patched:** Software manufacturers issue program updates containing *patches* to fix known vulnerabilities. Set *Microsoft Windows* and *Office* to automatically update. Manually update other programs like Adobe Acrobat, iTunes, Flash and Java. We list available updates for some of the more common programs in our *Weekly Patch and Vulnerability Report*, available on our blog: http://blog.citadel-information.com.

2. **Limit Exposure:** Create separate accounts for all family members. This is done in the *Control Panel*. Set *account type* to “Limited” unless the account needs to run programs as “Administrator.” This will make it harder for cybercriminals to install malware on your computer.

3. **Protect Your Desktop:** Install a *reputable antivirus / antispyware product* & keep it up-to-date. If you’re technical, run *Firefox* with the *NoScript* add-on inside of *sandboxie* and install a *host intrusion prevention system*. Sophisticated cybercriminals can get past basic antivirus/antispyware software. Antivirus is necessary. It is not sufficient.

4. **Secure Your WiFi:** If you have a wireless network, encrypt it with WPA2 encryption. Otherwise anyone near you can eavesdrop on your communications and piggy-back on your connection.

5. **Stay Away from P2P Networks:** Don’t run Peer-to-Peer or other file sharing programs, such as *Kazaa*, *Limewire* or *BitTorrent*. These networks provide strangers access to your computer.

6. **Beware of Scams, 1:** Don’t click on web-site ads or pop-ups offering to scan your computer for free. Cybercriminals love to take advantage of people’s fear of getting a virus. Instead of scanning your computer, these programs will infect it. Always be wary.

7. **Beware of Scams, 2:** Don’t open unusual or unexpected attachments, not even from people you know. It’s easy to send an email so it looks like it came from someone else. Also, how do you know your friend’s computer hasn’t been taken over? Always be wary.

8. **Beware of Scams, 3:** Don’t follow links in unfamiliar or unusual emails, especially those requesting your user names, passwords, or financial information. A SPAM filter can help you avoid these e-mails but you must be on guard for emails that get past your SPAM filter. Always be wary.

The Guide provides more than a dozen additional recommendations, covering five different defense strategies. Many of them are also free.

Most important, perhaps is the opportunity your question gives to seeing information security from a different point-of-view, replacing the question “what is the possibility of my personal computer being affected” with the far more practical — and also deeper — question “what can I be doing better to keep malware off of my computer?”

I encourage you to keep this question in your mind as you use your computer. The Department of Homeland Security has a public relations campaign to encourage consumers to do just this. It’s called Stop. Think. Connect.

Reprinted from our blog: www.Citadel-information.com/blog