Frequently Asked Questions on Computer Security
by The Henry County Bank

Q: Do I have to buy expensive software to clean viruses from my computer?

A: There are reputable programs available for free on the internet that may meet your needs. Be sure to do your homework prior to installing any software. Verify the software's reputation using software review websites such as Cnet.com, prior to installing the software. Some examples of free anti-virus protection and malware removal are:

Program	Web Address
Avast! Home Edition	http://www.avast.com/
AVG	http://free.avg.com/
Malwarebytes	http://www.malwarebytes.org/
Microsoft Security Essentials	http://www.microsoft.com/Security_Essentials/

Note: We cannot endorse or recommend any of the above programs. They are listed here only to show examples of what is available.

Q: Is one anti-virus software program better than another?

A: Marketing hype aside, all reputable antivirus software does pretty much the same job. Some may be better than others in regards to a particular feature, but any one of them is better than no antivirus software at all. However, there are a number of disreputable antivirus programs that actually do more harm than good. Be wary of any antivirus software that advertizes itself via unsolicited e-mail (spam) or pop-up windows.

Q: How do I know if my PC is infected?

A: Infected PCs may exhibit suspicious behavior, such as running more slowly than normal, locking up often, crashing and restarting frequently, or displaying unusual error messages. Or they may exhibit no symptoms at all. Also, the suspicious behavior often shown by infected PCs may be caused by a number of other factors. So while a poorly performing computer should make you suspect that it may be infected, you won't know for sure unless you frequently scan your PC with an antivirus tool.

Q: Aren't you safe from these threats if you stay away from those shady and unsavory websites?

A: Your PC could be infected from a number of sources. Viruses can be transferred from PC to PC through the use of a shared USB Flash Drive. There are many instances where a nationally recognized company's website has been compromised and visitors to their site have been infected with malware. The best way to protect yourself is to protect your PC.

Q: What do I need to do to protect my PC?

A: While there is no silver bullet that will protect you from every risk, if you take the following precautions, you can significantly reduce your exposure:

- Install an antivirus program and configure it to update its virus definitions daily.
- Configure your computer and connection to the internet properly. Some computer systems come with a lot of security enabled by default, but have someone who knows what they're

doing check the configuration of your computer and other communications equipment — wireless routers, DSL or cable modems, etc.

- Turn on automatic software updates. This is a feature of some software which allows it to patch itself with very little effort from you. Make sure it's turned on for your operating system, security software, and any applications that have the option.
- Be aware of your Internet surroundings. Learn to tell scams from real email, and when not to follow links or open a document. It takes time and practice to develop Internet “street smarts.”
- Perform regular backups. If your system becomes infected with a virus, you may have to reinstall your complete system. Backups ensure you don't lose your data if that becomes necessary.