Very few companies' online banking is secure. We strive to make sure *our* clients are not one of those companies, Are you aware of the dangers of not having a single secured computer that is used just for online banking?

The following statements from Clark Howard's website explains the reason you need to secure your online banking -

"If you're an individual and your computer is breached, you have protections under the law and your money must be restored to you. But that's not the case if you're a business owner. That's why entrepreneurs need to follow my advice carefully. ***If you're a business owner, you must have a dedicated computer that's only used for financial transactions****."*

In other words, **if money is illegally removed from a business account, you have no recourse. The money is gone.**

What can happen on computers that are not secured? Software that captures every keystroke as well as screen shots can be installed without you ever knowing it. These programs are referred to as Keylogger software.

There are many ways your computer can get infected with Key logger software:

- It can be bundled with other software that is downloaded. (When downloading software, especially freeware, we recommend using cnet.com or download.cnet.com if possible.)

- Deceptive pop-up ads could be links to fake websites.

- Fake Windows notification pop up messages. Some may have buttons such as Yes and No. Clicking on either button will download and install the software.

- When doing a Google or Bing search, clicking on a link could bring you to a Phishing site. (This is a good link to learn about Phishing. Note the section "**Beware of links in email."** **http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx)**

So why do you need this extra security for online banking when you have protection in the form of Antivirus software and a secure firewall? The Antivirus

software does a good job blocking many viruses, however it can take days before *any* Antivirus software catches up to the latest viruses and spyware.

This is a very good article explaining some of the ways people are tricked into installing spyware. Rouge Antivirus

What can we do about it?

- Setup a single computer, preferably in a secure room, that is used only for banking.

- Isolate the computer from all other computers on the network by creating a separate network. This is done inside the corporate Firewall.

- The only programs installed are ones needed for online banking along with Adobe and Antivirus software.

- Lock down internet access from the computer so it can only get to banking sites, Microsoft for updates, AntiVirus for updated signature files and to bnsatl.com for remote support.

For added security inside the office if needed:

- Place the computer in a secure room. Remote access to the computer can be allowed from a single computer inside the network.
- Disable ability to write to USB storage devices and CD Rom.

What do you need?

- A computer to dedicate to online banking.
- SonicWall Firewall.

If you are interested in setting up secure internet banking, call us anytime 404-446-3330.