Access to information and entertainment, credit and financial services, products from every corner of the world — even to your work — is greater than ever. Thanks to the Internet, you can conduct your banking, purchase products, get expert advice in an instant, or collaborate with co-workers in a "virtual" office.

But the Internet — and the anonymity it affords — also can give online scammers, hackers, and identity thieves access to your computer, personal information, finances, and more.

With awareness as your safety net, you can minimize the chance of an Internet mishap. Being on guard online helps you protect your information, your computer, and your money.

To an identity thief, your personal information can provide instant access to your financial accounts, your credit record, and other assets. If you think no one would be interested in YOUR personal information, think again. ANYONE can be a victim of identity theft. In fact, according to the Federal Trade Commission, millions of people become victims every year. Visit ftc.gov/idtheft to learn what to do if your identity is stolen or your personal or financial information has been compromised – online or in the "real" world.

When you listen to the news, you hear about many different forms of computer infection(s). The most common are:

- **Viruses** - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.

- **Malware** - Malware will perform a variety of unwanted functions, ranging from simple e-mail advertising all the way to complex identity-theft and password stealing. New functions are created every week by malware programmers.

- **E-mail viruses** - An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.

- **Trojan Horses** - A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.

- **Worms** - A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

- **KeyLogger** - A KeyLogger is a computer program that logs each keystroke a user types on a keyboard and saves this data into a file or transfers it via the Internet to a predetermined remote host. It also can capture screenshots of user activity, log passwords, record online chat conversations or take different actions in order to find out what a user is doing.

Current Trends:

- Over 86% of e-mail is spam (FTC)
- 1 in 148 e-mails is a virus / Trojan (MessageLabs)
- 3 in 100 PCs contain ID Theft Trojans (Panda Labs)
- 52% of new viruses last only 24 hours (Panda Labs)
- 90% of people are fooled by a well constructed Phishing attempt (Harvard & University of California)
- 59 million users in the US have spyware or other types of malware on their computers (*Consumer Reports WebWatch)*
- The number of computers infected with malware designed to steal personal and financial information has risen 600% in the last year (Panda Labs)

COMPUTER VIRUSES:

Preventing a viral infection of your computer is much easier than eliminating one you have already contracted.

- **Avoid Unknown Attachments**. Nowadays, most viruses are spread via e-mail attachments which, thankfully, can only become active when the attachment is opened or unzipped. While you cannot contract a virus just by receiving e-mail, it is a good idea to delete messages containing attachments if you do not know the sender, or if the subject line includes a tempting phrase like “Here is the file I promised you.”

- **Avoid Bootleg or Pirated Software**. With popular software packages running upwards of $200, it can be hard to resist the lure of the bootleg versions freely available on Internet file sharing sites.

- **Back It Up**. Along with hardware failure, theft and acts of God or Nature, the possibility of viral infection is just one more reason to back up your data regularly. You should always keep the last and the next-to-the-last backups in case you need to restore files that have been corrupted.

- **Purchase Antivirus Software** (*there are free utilities available as well*). Most antivirus software packages offer an automatic background protection mode, which will detect and clean out infections as they appear.

MALWARE:

Malware will perform a variety of unwanted functions, ranging from simple e-mail advertising all the way to complex identity-theft and password stealing. New functions are created every week by malware programmers, but the most common malware functions are:

- Malware steals your personal information and address book (identity theft and keystroke logging).
- Malware floods your browser with popup advertising.
- Malware spams your inbox with advertising e-mail.
- Malware slows down your Internet connection.
- Malware hijacks your browser and redirects you to an advertising or a phishing-con web page.
- Malware uses your computer as a secret server to broadcast pornography files.
- Malware slows down or crashes your computer.

PROTECTING YOURSELF AND YOUR SYSTEMS FROM SPYWARE / MALWARE:

Install two or three different antispyware programs ("spyware cleaners") on your computer, and update their definition lists regularly. Because every antispyware cleaner is imperfect, it is necessary to use combinations of these programs to catch the greatest breadth of malware. Also, the antispyware manufacturers regularly add new entries to their "definition" lists, just like antivirus software. Make sure to keep your spyware cleaners updated with these lists!

Build a weekly habit of "scan and detect". Like cleaning house, this should be done every few days. At the very least, this should be done whenever you install new software. Many antispyware programs can be set to automatically perform scan and detect nightly.

Carefully read every EULA (end user license agreement) before clicking "accept". If you see the phrase "Third party software may be installed", make sure to follow the software install with a spyware cleaning. Ask yourself before you install a program, “Do I REALLY need/want this program?”

Educate yourself on the latest strains of malware. In particular, start visiting these recommended antispyware sites, and update yourself on the latest malicious programs.

Save your data, and backup often! In other words, "prepare for the worst". Backing up means: *keep your original software CDs in a safe accessible place, constantly save copies of your important work files on CD or separate drives, and presume you will actually need them one day.* This way, if you ever experience the extreme spyware circumstance of having to reformat your hard drive, you can at least recover your important work and/or files.

KEYLOGGERS:

What is a KeyLogger?

A KeyLogger is a computer program that logs each keystroke a user types on a keyboard and saves this data into a file or transfers it via the Internet to a predetermined remote host. It also can capture screenshots of user activity, log passwords, record online chat conversations or take different actions in order to find out what a user is doing. A KeyLogger poses the most dangerous threat to user privacy.

How does your computer become infected?

KeyLoggers differ from regular computer viruses. They do not spread by themselves and usually must be installed as any other software with or without user content. There are two major ways unsolicited keystroke logging program can get into the system.

- A legitimate KeyLogger can be manually installed by system administrator or any other user who has sufficient privileges for the software installation. A hacker can break into the system and setup its own KeyLogger. In both cases a privacy threat gets installed without the monitored user's knowledge and consent.

- Malicious KeyLoggers often are installed by other parasites like viruses, trojans, backdoors, or even spyware. They get into the system without user knowledge and affect everybody who uses a compromised computer. Such KeyLoggers do not have any uninstall functions and can be controlled only by their authors or attackers.

What does a KeyLogger do?

- Logs each keystroke a user types on a computer's keyboard.
- Takes screenshots of user activity at predetermined time intervals or when a user types a character or clicks a mouse button.
- Tracks user activity by logging window titles, names of launched applications, exact time of certain event occurrence and other specific information.
- Monitors online activity by recording addresses of visited web sites, taken actions, entered keywords, and other similar data.

- Records login names, details of various accounts, credit card numbers, and passwords including those hidden by asterisks or blank space.

- Captures online chat conversations made in popular chat programs or instant messengers.

- Makes unauthorized copies of outgoing and incoming e-mail messages.

- Saves all collected information into a file on a hard disk, then silently sends this file to a configurable e-mail address, uploads it to a predefined FTP server or transfers it through a background Internet connection to a remote host. Gathered data can be encrypted.

- Complicates its detection and removal by hiding active processes and concealing installed files. The uninstaller, if it exists, usually refuses to work if a user cannot specify a password.

How to remove a KeyLogger?

Most KeyLoggers work in the same manner as the computer viruses and therefore can be found and removed with the help of effective antivirus products.

PATCH YOUR COMPUTER:

One of the single most important actions you can do to your computer to protect it is to ensure that your operating system and critical programs are up-to-date.

Each second Tuesday of each month, Microsoft releases new patches for all of their products affected by security or reliability problems.

Hackers find ways to get into Windows by finding flaws affecting assorted areas of your operating system. If you do not fix those flaws, some hackers could get in your system using these security holes. Even viruses can use these holes to try and get into your computer.

Having an anti-virus doesn’t necessarily mean that you are protected against all threats! Sometimes, a virus can move around quite a bit before security companies get the anti-virus definition out to their customers.

Remember – It’s Your Data/Information: Protect It.

While WaterStone Bank does not endorse or recommend specific computer maintenance or security products, below is a list of available products that have proven effective in protecting computers systems from the issues discussed above. You are encouraged to research and use whichever product you feel best suits your needs and budget. *(This is only a sample of available products)*

Anti-Virus Applications:

- Symantec/Norton
- McAffee
- AVG
- Kaspersky
- Trend-Mirco
- Avira

Malware/Spyware Applications:

- Spy-Bot
- Ad-Aware
- MalwareBytes
- Spyware Blaster
- Symantec/Norton
- Spyware Doctor
- SpySweeper