

About Swiftec IT

Swiftec IT is a full service IT services company in the heart of MetroWest Massachusetts. We are here for our customers with a simple but critical mission: To bring corporate IT quality and sophistication to small, midsize and growing companies that don't want to commit the time, capital and resources required for a full time IT staff and department. Let us help you grow and succeed in today's dynamic and changing digital business world.



Swiftec IT was founded by IT industry leader Adam Winter. Adam brings the global experience of major corporations he served to smaller companies where it can have significant and immediate impact. He is noted for insights and solutions to computer problems that beset many companies: business continuance, training, disaster recovery, creating help desks and other vital IT functions.

Swiftec IT brings an inside understanding of the needs and requirements of the most competitive industry categories: Financial services, insurance, publishing, manufacturing, contract services, consulting, and non-profit enterprises. Our learning and insights in these and related industries can bring new perspective to your specific problems and IT challenges.

DELL™ reseller

Computers & Fileservers

Computer / network

design & installation

Web site design / hosting

on our dedicated server

Automated Remote Backups

offsite, secure, piece of mind

Protecting Your Information



*Internet Security and Safety
for you and your family*

Presented by:

Adam Winter
President
Swiftec IT, Inc
292 Main St
Northborough, MA 01532

Today, information is truly “at your fingertips”.

Unfortunately, there are predators and thieves who are computer savvy and want to utilize this amazing technology to their advantage.



These few pages are designed to help you “surf” the Internet safely. The flow of this document will start with the connection to the internet and work towards the person behind the keyboard.

Firewall

A firewall is your first line of defense. It makes your computer invisible (stealth) to the Internet to protect you from intruders who are random dialing for people without firewalls.



A firewall can be either a piece of hardware or software. Examples of a hardware firewalls are the Linksys, Netgear, or Dlink routers you can purchase in many stores. Software firewalls are available with most Anti-Virus software as well as built into Windows. We strongly suggest turning OFF your software firewall and using a hardware firewall! (This comes from years of experience and frustration.)

Wireless Internet

Wireless connections are great. They allow you to connect to the internet from the family room, the conference room, the pool, or the pool hall. The way a wireless access point (WAP) works is that it BROADCASTS its availability to anyone within ~300 feet. Think of the broadcast as a welcome mat for your neighbors or anyone driving by to connect to your network. This type of access gives anyone direct access to your computers, so you want this to be secured. It is **CRITICAL** that you protect your WAP with security. The



Swiftec supports our community!

Members of our team support the following organizations with their time, skills or donations:

Home Safety Network.....	http://homesafetynetwork.org
Northborough Rotary.....	http://northboroughrotary.org
Westborough Rotary	http://westboroughrotary.org
W'boro Spring Festival.....	http://spring-festival.com
North East Link.....	http://northeastlink.org
Northborough Family League.....	http://northboroughfamilyleague.com
Northborough Free Library.....	http://www.northboroughlibrary.org
Congregation B'nai Shalom.....	http://cbnaishalom.org
Corridor Nine Chamber of Commerce..	http://corridormine.org
Blackstone Valley Chamber of Commerce	http://blackstonevalley.org
Algonquin Boosters	
Northborough Basketball	

Our newsletter

Interested in monthly computer tips? Sign up for our newsletter at: <http://swiftecit.com> – click on Sign up for our newsletter in the yellow box.

Prior month’s newsletters can be found at <http://swiftecit.com/news>

blocked. While you can override the restriction for that web page, you will have to override it for each instance – which will drive you crazy.

Protecting your children – option 2



An alternative to blocking sites, is to monitor what websites the computer has been to. Try the following to bring up your Internet browser's history:

For Internet Explorer 6.x – click CTRL-H
For Internet Explorer 7.x – click Ctrl-Shift-H
For Firefox – click CTRL-H

What you will see are the web sites this computer has been to in the last 20 days. What we now suggest (after dealing with the “Parental control” software), is that you let your children know that you can check where they have been and that if the history is NOT there – then there will be consequences.

We hope this information has been helpful to you. If you are interested in other local organizations who help children please look at the next page of some of the organizations we are involved with.

simplest to implement is called WEP. While this can be cracked, don't worry about it unless you have national secrets to protect. It will prevent people from accessing your network – which is the goal.

Computer Software

The one piece of software you must have on your computer is Anti-virus software. Of the choices available, we prefer a product called Trend Micro Pc-cillin. This is the easiest to configure and does not slow down your computer.



A good piece of anti-virus software will have email filtering (for spam), spyware protection (another type of virus), and “Parental Controls” which will be discussed further on.

Spam protection

Spam is unwanted, unsolicited, mass distributed emails. You will notice on newsletters there is an unsubscribe option on the bottom of the newsletter. **Be careful!** The SPAM emails now have the same type of unsubscribe verbiage, but instead of removing you from their list – they ADD you to even more lists.



How do you know what is bad spam and nuisance spam? Look at the “from” address – is it a real company, can you go to their web site? If so, you can safely unsubscribe. If you cannot find their web site, then consider them “bad” spam and block them from your email.

Spam can be blocked several ways:

- At the server – whomever you get your email from may have the option of filtering spam. Some of these solutions have proven to be excellent.

- At your computer #1 - Microsoft Outlook has a spam filter which will put spam into a designated folder. The sensitivity of the filter can be set by you. We have found this to be so-so.
- At your computer #2 – Third party software has the ability to filter spam as well. Generally this is better than Outlook, but not as good as filtering on the server.

Best Email Practices



The best piece of advice we can give to you is – if you don't recognize the sender of the email – **DON'T OPEN THE ATTACHMENT!** This is how most people get infected by viruses, spyware, or other destructive software. Your action of opening the attachment opens the door for you to be infected (you are granting the program access to your machine). Here are some of the types of scams out there.

- Phishing - the practice of luring unsuspecting Internet users to a fake Web site by using authentic-looking email with the real organization's logo, in an attempt to steal passwords, financial or personal information, or introduce a virus attack.
- You have received an e-card from a high school friend – there are a number of versions of these emails sending either pdf's or invitations to view an electronic card. The best choice is to use your delete button.

If an email has a hyperlink, check the following:

- Hover over the link. Does it point to a number (i.e. 66.55.231.2)? If so, delete the email.
- Do you recognize the web address you want to go to? ebay.somesite.com is not the same as www.ebay.com. The first is a fraudulent website.
- Are you being asked for any personal information? If so, use the phone if you want to provide the information.

Protecting your children – email

We have recently started using software that blind copies a specified person on all emails. This will allow you to monitor any outgoing correspondence from a given computer.

Our current use of this software is limited to the financial industry that requires copies of all correspondence, but the same software could be used to monitor children's email.

Protecting your children



Computer software is only part of the solution for protecting your solution and it may not be the best alternative. We recommend that the computer children use is in a public part of the house; a family room, kitchen or somewhere that does not have a closed door. The fact that you may walk by at any given time is a powerful deterrent.

For the times when you are not around, there are two other options to consider. The first option is software which provides "Parental Controls". The antivirus software we recommended above (Pc-cillin) has this capability built in, so you don't need additional software.

Many web sites are encoded with ratings – similar to the movie rating code for sex and violence, but ratings are not required on all sites. Parental controls will restrict access to the types of sites you specify (sex, horror, politics, instant messenger, nudity, etc). If someone tries to access an unauthorized site, actions range from an email sent to you immediately to a pop-up asking for an override code.

While the software has good intentions, we have found it to cause more of an issue than not having any software. When a research paper needs to be done on the Aborigines, or American History – you may come across legitimate sites for research which are now