Protect My Computer

FIREWALLS

1–Identify if your modem or router has a built-in firewall

Visit your router or modem manufacturer's support Web site and type in the model number to determine if it has a built-in firewall. The support Web address for the major manufacturer's are: ❶ Cisco Linksys or Valet - homesupport.cisco.com/en-us/support ❷ D-Link - dlink.com/support ❸ NETGEAR - kb.netgear.com ❹ Belkin - en-us-support.belkin.com.

2–Enable the firewall within your router

Your router's firewall settings can be accessed through your Internet browser by entering in the router's **URL** or **IP address**. This information is usually found either on the router itself, in the packaging materials, or on the manufacturer's support site.

Protect My Computer

FIREWALLS

3–Create a strong admin password for your router

Change the **administrator** password (not user) to a strong password after logging in to your router for the first time. For guidelines on setting a strong password, reference the **Protect Myself** worksheet.

4–Create a strong wireless network password

It is a good idea to choose a different password to join your network since you may want to allow guests and others to connect to your wireless network without giving them access to change the router's settings.guidelines on setting a strong password, reference the **Protect Myself** worksheet.

Protect My Computer

PHYSICAL SECURITY

1–Store your sensitive information away from home

Important documents such as birth certificates, deeds, tax returns, contracts, bonds, or other important items should be stored in a safety deposit box.

2–Shred all unnecessary documents

Divide documents into groups such as: ❶ **SHRED NOW** - Unsolicited credit card offers, expired credit cards, old passports and driver's licenses. ❷ **SHRED MONTHLY** - Credit/Debit card receipts after being reconciled. ❸ **SHRED YEARLY** - Monthly statements after reconciling with year-end statements. ❹ **SHRED ON A SEVEN TO TEN YEAR BASIS** - Year-end bank statements over 7 years old, titles and deeds to property you haven't owned in seven years.

3–Protect all digital storage devices

Never leave these items in your car, Avoid leaving them in plain view through a window in your house, and consider keeping DVD's or hard drives with computer back-ups in a safe or safety deposit box.

Protect My Computer

UPDATES

1–Regularly update your operating system (OS)

Most PCs include an update program, such as Microsoft's Windows Update, that is set to automatically check for OS updates. It is important to install these updates as soon as possible after receiving notification that they are available.

2–Check for updates on all of your computer applications

Non-OS programs such as Adobe Photoshop and Quicken will not update through the OS update software. Many can be configured to check for updates when the program is opened. Most have a 'Check for Updates' button under the Help menu.

Protect My Computer

SECURITY SOFTWARE

1–Configure your antivirus software to update itself

Look for a setting in your antivirus program that says update virus signature database or similar wording. If the last update is not within the last few days, manually update it to ensure your computer has the latest security updates.

2–Keep your antivirus license current

The license status of your antivirus software is usually found by clicking the 'About' button under the Help menu. Make sure to check when the license is valid till so you can purchase a new license before it expires.

3–Call your antivirus tech support if you have questions

The tech support number can be found on the company's support Web site or in the packaging materials. Many antivirus companies charge for tech support, but some are free such as ESET.

Protect Myself

EMAIL

1–Add friends to a safe senders list

To block or allow an e-mail address using Microsoft Outlook, right click the e-mail address and select > **Junk E-mail** > **Add Sender to Blocked Senders List** OR **Add Sender to Safe Senders List**.

2–Check the URL address of links before clicking on them

While the text of the link may look like a valid website, the actual link may be very different. Always hover your cursor over the link for a moment until a yellow box appears showing the actual link. If it is different than what you expected, Do not click on it.

3–Confirm the sender before clicking on Links in an email

The safest way to avoid malicious links is to type in the address manually in your browser or select the website from your saved bookmarks.

4–Keep identity-rich personal info out of email

Since email can easily be forwarded on to anyone or intercepted by someone other than the intended recipient, DO NOT put personal information in an email. This includes credit cards numbers, social security numbers, bank account information, etc.

Protect Myself

INTERNET USAGE

1–Use only secure and private connections (https)

Make sure a website begins with **https**, instead of just http when entering personal information. The 's' means the information you enter will be encrypted so that it can only be understood by the intended recipient, such as your bank.

2–Keep ALL vital personal information private

Entering in just your birth date or social security number on another site may seem harmless, but cybercriminals can combine this information with pieces of your identity available from other unsecured sources. For this reason, do not submit this info.

3–Check a link's authenticity before clicking on it

To check a link, hover over the link without clicking on it and you will see the actual Web address at the bottom of the window in your Web browser. If you don't see a status bar at the bottom in Internet Explorer, go to **View > Toolbars > Status Bar.**

PASSWORDS

1–Create strong passwords on your online accounts

Consider these tips:

1. Combine words (blind MICE = bMIliCnEd)
2. Use an acronym (I Shower Every Week Or So = i$ew0s)
3. Use numbers and symbols in your passwords, and unorthodox caPitALizAtiOn

Avoid these pitfalls:

1. Any part of your name, or any name in your family, birthdates, anniversaries, etc.
2. Song titles, famous people, or any correctly spelled word
3. Keyboard combinations such as 123456, qwerty, abc123, etc

PASSWORDS

2–Change your passwords every six months

Changing your passwords frequently will help keep cybercriminals from discovering them.

3–Use a different password for each account

Using the same password for every account means that if it is cracked once, every account is in danger. Keeping them different can stop the 'wildfire' from spreading.

4–Store your passwords in a safe location

If you have trouble remembering your passwords, consider an online password service to help keep track of them. These services store all your passwords securely and integrate with your other devices. Examples: 1Password, mSecure and SplashID.

Protect Myself

SOCIAL NETWORKING

1–Enable strict privacy settings on your networking sites

Change the privacy settings on your social networking sites to *ONLY share information with friends and family*. The more strict your settings, the more difficult it is for someone with ill intent to get a hold of this information.

2–Screen the people you link before granting access

Avoid linking to anyone you don't know. Even those you do know, limit the information available to them. Consider creating different groups: one for close friends, one for family, and one for others. Then set up how much information is available to each group, and choose which groups will see your updates.

3–Think twice before sharing information

Even if you post information for just a moment, that's enough time for someone to save it to their computer. Ask yourself if you'd feel okay if an image was seen by your employer or family, or the employers and families of anyone else in the photo.

4–Limit sharing too many details

While it's easy to post comments publicly about every detail of your life, or your GPS location, this can often put you in danger. If it's publicly known that you aren't at home, you could be a target of physical theft since a criminal knows you are away.

Protect My Family

CYBERBULLYING

1–Choose age appropriate social networking sites for your kids

Sites such as Facebook and MySpace automatically collect personal information, so young children are legally not allowed on them. Instead try these age appropriate sites: whatswhat.me, togetherville.com, imbee.com, and gianthello.com.

2–Stress the importance of personal information online

Even if information is deleted from a site, your children have no control over older versions that exist on other people's computers and circulate online. That's why it is important to sit down with them and explain that they need to think twice before posting anything online that the whole world could see.

3–Monitor your children's social networking activities

Most social networking sites include a '*wall*' which lists the entire history of all posts on your child's profile, and is an easy way to monitor their activity. There is also usually a feature to save all chat messaging to a history which you can review later.

Protect My Family

PARENTAL CONTROLS

1–Set up parental controls included with your computer

Pre-installed parental controls typically can limit when your kids can use their computer and restrict what desktop programs they can use. Microsoft Windows parental controls are located by going to > **Start** > **Control Panel** > **Parental Controls**. Remember to set a strong password that only you know, when setting up the parental controls.

2–Consider additional software for more advanced control

Advanced parental control software can restrict personal information sent out to other sites, filter content in Web pages, and monitor activity of when and where your kids spend their time online. Advanced parental control programs include: Net Nanny, CyberPatrol, and K9 Web Protection.

Protect My Family

INTERNET USAGE FOR KIDS

1–Keep computers within sight to monitor activity

Even with filtering and monitoring software installed, the Internet is still a dangerous place for children. Make sure that you can see their screen and what they are doing. It is also a good idea to periodically check in or join them in their online activities.

2–Establish rules for computer usage

Age appropriate rules include:

1. Restrict nighttime usage
2. Limit the total number of hours in a given day/week
3. Ban chatting with strangers
4. Require approval before 'befriending' someone online

3–Establish rules for mobile phone usage

In addition to the rules above:

1. Limit the number of minutes and texts used each month
2. Ban usage when doing homework
3. Require approval for all contacts in their phone book