Make Backups

Backup all important folders, files and information at least once a week. Just as you protect your irreplaceable valuables protect files that cannot be replaced by performing a backup. Don't forget to keep backups in a safe place.

Use Care when Downloading or Installing Programs

Buy software and programs from vendors that you trust or are well known nationally. Learn about the software or program before purchasing or downloading. Use software that has been safely used by others or recommended by a knowledgeable, trusted individual.

Establish Security Guidelines

Create a family contract with clear rules for using the computer and the internet. Keep a list of internet access guidelines and good computing practices close to your home computer for all to see. Stay aware of the security aspects of any technology or software used at home, learn associated threats and how to handle them. Share this information with the entire family.

Wireless Security

Research your specific wireless hardware vendor's recommendations on security. Change the default password on the router. Enable MAC address filtering to limit network access to specific machines. Use the highest level of security offered by your device. i.e. WPA2, WPA, WEP. Change the default SSID and do not broadcast it out to the public.

PROTECT YOUR CHILDREN ONLINE

Although software can help you protect your family from inappropriate content on the Web, there is no substitute for teaching your children a few basic rules.

-Teach your child to never give personal information to anyone online.

-Teach your child to not trust people online that they do not know personally.

-Know your children's online friends.

-Keep the family computer in a centrally-located place in your home.

-Stay informed of cyber-related threats against children and protective measures to be taken

-Implement Parental Controls.

-Provide separate user accounts for each child and control their access.

-Consider installing software that allows you to monitor your child's activity on the internet.

Useful links:
www.cert.org/homeusers/HomeComputerSecurity

CYBER SECURITY AT HOME

PROTECTING YOUR FAMILY

NAVY INFORMATION OPERATIONS COMMAND NORFOLK

What is Cyber Security?

Cyber Security is the set of principles and practices designed to teach you how to safeguard your computing assets and online information from threats. Communication and computing technology are the vehicles that we use to transport, exchange, extract and store all kinds of information. You probably use many kinds of current technology such as internet-connected computers, cell phones, personal digital assistants (PDAs), digital cable or satellite television. Technology is a part of everyday life so it is imperative that you learn to protect yourself and your family from cyber crimes by arming yourself with cyber security knowledge.

What could happen?

By allowing our children to use these sophisticated tools without proper training and preparation or with no warning against the dangers, it is no surprise that they will often inadvertently cause damage, expose themselves to inappropriate content, or encounter malicious individuals.

Useful links:
www.jtfgno.mil/antivirus/antivirus_homeuse.htm

Understand the Risks

Virus: Self-replicating code that spreads by inserting copies of itself into other software programs or documents

Trojan Horse: a malicious program disguised as legitimate software

Worm: a self-replicating, self-spreading malicious program

Spyware: software that sends information from your computer to a third party without your consent

Malware: programs designed to harm your computer

Intrusion: trying to gain privileged access to computer systems in order to steal, corrupt or illegitimately view data

Identity Theft: the theft of personal information to commit fraud

Steps to a Secure Network

CREATE STRONG PASSWORDS

-Use a unique password or passphrase

-Change it often

-A strong password consists of AT LEAST eight characters and should include letters, numbers, and special characters. Examples:

J*p2leO4>F.
H@rd2Cr@k!

-Do not write down your password, instead if you need to, write down a hint that will help remember it.

Anti-Virus and Anti-Spyware Software

Anti-virus and anti-spyware scans files in your computer's memory for certain patterns that may indicate an infection. They must be kept up to date. Even if you have it set to automatically install updates, check often to ensure the latest virus definitions are installed. The DoD Anti-Virus Software License Agreement with McAfee and Symantec allows active DoD employees to utilize the antivirus software for home use for free. Contact your commands local IT department for more information.

Use a Firewall

The firewall acts like a guard, keeping potentially dangerous files, requests, or programs from accessing your computer and it's resources. It can also be set to block or allow specific websites. Today, most of the popular operating systems used on home computers come with personal firewall software. Take the time to learn what yours has to offer.

Be Cautious of Emails with Attachments

Is the email from someone you know?
Have you received email from this sender before?
Were you expecting email with an attachment from this sender?
Does the subject and name of the attachment make sense?
Should you scan the attachment before opening it?
Web based email clients such as Yahoo and Hotmail often do not rely on your computers antivirus software to detect malicious files. Ensure your email client performs antivirus scans on your email before it's downloaded.
Additionally to protect yourself while using email, assume email from unknown senders is spam and don't forward chain letters.