How To Protect against threats

Secure Your Email

- Only open email attachments that come from a trusted source and that are expected
- Scan email attachments with Antivirus prior to opening
- Delete all unwanted messages without opening
- Keep security patches up to date Coverage
- If you suspect an email is spam, do not respond, just delete it
- Consider disabling the email's preview pane and reading emails in plain text
- Be extremely wary of emails asking for confidential information
- Confirm the authenticity of a suspicious request before responding in email

Browse the Web Safely

- When visiting a website, type the address directly into the browser rather than following a link
- Only provide personal information on sites that have "https" in the web address or have a lock icon at bottom of the browser
- Do not provide personal information to any unsolicited requests for information
- Allow only authorized programs to connect to the Web
- Do not accept or open suspicious error dialogs from within the browser
- Spyware may come as part of a "free deal" offer - Do not accept free deals
- Install product updates and security patches before using the internet
- Keep web browser up to date with latest patches
- Make sure your computer is configured securely
- Automatically shield newly discovered security holes

Safeguard Your Instant Messenger (IM)

- Don't open attachments or click on Web links sent by someone you don't know
- Don't send files over IM
- If a person on your Buddy list is sending strange messages, files, or web site links, terminate your IM session
- Remove viruses from IM with your Antivirus
- Reject all Instant Messages from persons who are not on your Buddy list
- Do not click on URL links within IM unless from a known source and expected
- Never send personal information through an IM
- Keep your IM software up to date
- Keep your operating system and security software up to date