To help protect you and your family from these cyber threats, the Stop.Think.Connect. Campaign offers the following advice:

STOP.

Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK.

Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety- or your family's.

CONNECT.

Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

STOP | THINK | CONNECT™

Protect yourself and help keep the web a safer place for everyone.

STOP | THINK | CONNECT™

Visit ***www.dhs.gov/stopthinkconnect*** for more information on how to get involved with the Stop.Think.Connect. Campaign.

SECURING ONE CITIZEN, ONE FAMILY, ONE NATION AGAINST CYBER THREATS.

MERRIMACK VALLEY REGIONAL TRANSIT AUTHORITY

www.dhs.gov/stopthinkconnect

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.

Cyber threats affecting you, your family, and members of your community include:

Identity Theft

- **Identity theft** is the illegal use of someone else's personal information in order to obtain money or credit.
- Identity theft can happen to anyone in any location across the country.
- Take simple steps to protect your online identity by:
  - Locking and password protecting your computer and cell phone.
  - Not sharing specific personal information online, such as your full name or birthday.
  - Setting proper privacy settings on social networking sites.

Fraud and Phishing

- **Fraud** is the intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right.
- **Phishing** is a scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.
- Fraud and phishing attacks may take the form of an authentic-looking website or a personalized email.
- Secure yourself from fraud and phishing attacks by:
  - Turning off the option to automatically download attachments.
  - Saving and scanning any attachments before opening them.
  - Before providing any kind of information, call and verify with the source that they are indeed the ones who sent the email.

Cyber Bullying and Ethics

- **Cyber bullying** is the electronic posting of mean-spirited messages about a person, often done anonymously.
- **Cyber ethics** help Internet users understand what type of online behavior is right and wrong.
- Cyber bullying and poor cyber ethics are threats many teens and young adults face not from strangers, but from their own peers.
- Whatever anyone posts online about another person can be spread virally, resulting in serious, unwarranted damage to an individual's reputation or personal well-being.
- If you are being bullied, report it to a trusted adult - a parent, teacher or neighbor.
- Avoid being a cyber bully and practice good cyber ethics by:
  - Following the Golden Rule - Be nice online and in real life.
  - Not saying or doing anything online that you wouldn't say or do in person.
  - Owning and taking responsibility for your actions online.

Cyber Predators

- **Cyber predators** are people who search online for other people in order to use, control, or harm them in some way.
- Cyber predators target teens and young adults - both male and female - on a regular basis, regardless of whether or not the victims are 18 or above.
- Social networking sites enhance a predator's ability to target young Americans, especially if they share personal information in their profile.
- To protect yourself from cyber predators:
  - Be aware - you never know who is behind the screen, so be protective of yourself and your personal information.
  - If you are being targeted or harassed online, notify your family or the proper authorities.