THE IMPORTANCE OF CYBERSECURITY

“The cyber threat is one of the most serious economic and national security challenges we face as a nation...America's economic prosperity in the 21st century will depend on cybersecurity.”
President Barack Obama

We live in a wired world. We use the internet to conduct business, communicate with friends, keep resources flowing and protect our public and private interests. Corporations, educational and financial institutions, medical networks, the nation’s power grids, military branches and national security all rely on cyberspace and cybersecurity to function properly.

Threats in cyberspace will soon equal or surpass that from terrorism. Cyber criminals and foreign adversaries look for ways to interrupt or destroy our financial and security systems everyday. Threats to shut down our power grids or water supply could paralyze our nation. Cyber attacks could bring our financial system to a standstill. Defense Secretary, Leon Panetta, recently warned that a devastating Cyber Pearl Harbor may well be imminent. Attacks from phishers and spammers trying to steal individuals’ information or expose them to spam are constant concerns for the internet user. The government, private sector and public must work together to improve our ability to detect and defend ourselves from cyber threats. Cybersecurity is everyone’s responsibility.

CHECK THESE OUT

http://www.staysafeonline.org/
National Cyber Security Alliance
Provides online safety tips for home, business, social media sites, etc.

http://stopthinkconnect.org/
National Security Council’s Stop/Think/Connect Program
Provides educational resources for Internet Security

http://www.whitehouse.gov/cybersecurity
National Security Council
Describes our nation’s cybersecurity strategy

http://www.dhs.gov/cybersecurity
U.S. Department of Homeland Security
Cybersecurity overview for the nation

spam@uce.gov
If you receive an email that may be a scam, forward it to the FTC and it will be stored in a database that law enforcement agencies use to generate legal cases.

http://www.ic3.gov/
The Internet Crime Complaint Center
To file a complaint regarding Internet crime

http://www.ists.dartmouth.edu/
Institute for Security, Technology and Society (ISTS)
at Dartmouth College. Research and education to advance information security & privacy

-------------------------
“The uncomfortable reality of our world today is that bits and bytes can be as threatening as bullets and bombs.”
General Martin Dempsey, Chairman of the Joint Chiefs of Staff

-------------------------
Program prepared by
Joseph Wiener
Millburn High School, Millburn, New Jersey
October 2012

Cybersecurity: Protecting Our Data
HOW TO PROTECT OURSELVES

Keep Your Equipment Clean
- Install the latest security software, web browser and operating system to fight against online threats. Allow for automatic software updates.
- Don’t forget to protect all devices that connect to the Internet. Smart phones, ipads, game consoles, and other web-enabled devices also need to be protected from viruses and malware.
- Use your security software to scan external devices such as USB’s when connecting them to your computer.

Keep Your Personal Information Personal
- Don’t just rely on your passwords to keep your accounts secure. Many service providers will let you set up extra security questions to prove your identity before allowing you access.
- Create more secure passwords using a combination of upper and lower case letters, numbers and symbols.
- Set up different passwords for each of your accounts to impede cyber theft.

Be Certain Before You Connect
- If a link seems suspicious, don’t connect to it. Links in emails, posts, advertisements, and tweets are ways cyber criminals compromise your software and equipment.
- Be smart about Wi-Fi hotspots. Adjust your security settings to limit who can access your computer, and limit the type of business you perform in hotspots.
- Keep your money safe. When shopping or banking online make sure the sites are secure. Look for web addresses with “https://” or “shttp://”, both are signs of sites that have taken the extra steps to keep your information secure. However, “http://” signals a site that is not secure.

Be Web Wise
- Keep abreast of the newest ways to stay safe online by checking trusted websites for the latest information.
- Stop and think before acting. Offers that sound too good usually are.
- Back up your work. Protect valuable information by making an electronic copy and storing it safely.

Be a Good Online Citizen.
- Your actions online have the potential to affect everyone. Practicing good online habits beneficial the entire digital community.
- Help the authorities battle cybercrime by reporting stolen records, finances, identities, and other cyber crimes to the correct authorities.

The above information was taken from the Department of Homeland Security’s Stop/Think/Connect Campaign.

DID YOU KNOW

20% of Americans report being a victim of a crime committed on the internet.

25% of Americans notified by a business, online service provider or organization that their identifiable information was lost or compromised because of a data breach.

59% of Americans say their job is dependent on a safe, secure internet.

THINKING ABOUT A CAREER IN CYBERSECURITY?

A recent Google search for Cybersecurity jobs resulted in a return of approximately 69,800,000 choices!

Benefits to a career in cybersecurity:
- The Internet Security field is expected to see strong employment growth over the next 10 years. Jobs in the cybersecurity field grew by 19% from 2011 to 2012.
- Provides good wages. The average wage was $82,000 in 2011*.
- Positions are needed in all geographic areas.
- Can work in a variety of settings such as software companies, design firms, financial companies, government jobs, hospitals, educational institutions, etc.

Some of the jobs available for those interested in a career in cybersecurity: (taken from the U.S. Department of Homeland Security’s website)
- System and Network Penetration Tester
  Assesses how well the systems and networks can withstand a sophisticated attack by adversaries.
- Application Penetration Tester
  Test applications before they are put to use. Identify the flaws with the system or network being tested.
- Incident Responder
  Implements measures to contain an incident and reverse its adverse effects.
- Threat Analyst/Counter-Intelligence Analyst
  Explore the ever changing technical vulnerabilities of the current system. Understand the attacker’s motivation, language, organization and social behaviors to create cyber profiles.
- Secure Coder and Code Reviewer
  Write code that is free of known coding flaws and of weak design approaches. Check software to find flaws and fix any flaws that are found.
- Risk Assessment Engineers
  Develop estimates of the risks associated with new technologies and newly discovered threats, so businesses can respond effectively.

*U.S. Bureau of Labor Statistics