

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government



DTI eSecurity News - Why Cyber Security is Important

What is a Cyber Security?

More and more of our everyday activities at work, school, and home involve computers and the Internet.



These cyber activities involve:

- **Communication** (email, cell phone)
- **Entertainment** (digital cable, MP3)
- **Transportation** (cars, navigation, airplanes)
- **Shopping** (online, credit cards)
- **Health** (equipment, medical records)

Cyber security is the protection of data and systems in networks that are connected to the Internet. The FBI ranks cyber crime as the 3rd greatest threat to United States National Security, just after nuclear war and weapons of mass destruction. These factors create an environment where vigilance is required, on a daily basis, to help mitigate risks.

Top Ten Cyber Security Tips

1. Turn on automatic updates in your firewall, anti-virus, and anti-spyware programs to ensure they are always up to date.
2. Verify that operating systems, browsers, and other software programs are properly setup and patched.
3. Employ password and authentication methods.
4. Configure computers to lock after a short period of inactivity.
5. Store important files on network drives, so they are backed up regularly.
6. Use extra caution and vigilance when browsing the Internet.
7. Maintain system security through repairs, upgrades, and replacements.
8. Remember that cyber security is everyone's responsibility!

What are the Risks?

The volume and complexity of cyber threats continue to increase. Below are examples of risks:

- Malicious code that erases all of your data files
- Someone breaking into the system and altering files
- Someone using your computer to attack others
- Someone stealing credit card information and making unauthorized purchases
- A collection of software robots, called botnets, unknowingly planted on your computer
- A virus that infects your computer and sends SPAM email to everyone in your contacts file

Recognizing Risks

The first step in protecting against cyber threats is to become familiar with the terminology.

Hackers, attackers, or intruders: People who seek to exploit weaknesses, in software and computer systems, for their own gain



Viruses: Requires something to actually be done before a computer becomes infected; such as opening an email attachment or going to a particular web page



Worms: Typically start by exploiting a software vulnerability. Then, once the victim computer has been infected, the worm will attempt to find and infect other computers on your home network.



Trojan horses: Software that claims to be one thing while, in fact, is doing something different behind the scenes. For example, a program that claims it will speed up the computer may actually be sending confidential information to a remote intruder.



Produced in part by US-CERT

Questions or comments?
E-mail us at eSecurity@state.de.us