Security Tip (ST04-001)

TLP:WHITE

Why is Cyber Security a Problem?

Original release date: May 06, 2009 | Last revised: February 06, 2013

What is cyber security?

It seems that everything relies on computers and the internet now — communication (email, cellphones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system?

You've heard the news stories about credit card numbers being stolen and email viruses spreading. Maybe you've even been a victim yourself. One of the best defenses is understanding the risks, what some of the basic terms mean, and what you can do to protect yourself against them.

Cyber security involves protecting that information by preventing, detecting, and responding to attacks.

What are the risks?

There are many risks, some more serious than others. Among these dangers are viruses erasing your entire system, someone breaking into your system and altering files, someone using your computer to attack others, or someone stealing your credit card information and making unauthorized purchases. Unfortunately, there's no 100% guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances.

What can you do?

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.

- Hacker, attacker, or intruder - These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting. The results can range from mere mischief (creating a virus with no intentionally negative impact) to malicious activity (stealing or altering information).
- Malicious code - Malicious code, sometimes called malware, is a broad category that includes any code that could be used to attack your computer. Malicious code can have the following characteristics:
  - It might require you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.
  - Some forms propagate without user intervention and typically start by exploiting a software vulnerability. Once the victim computer has been infected, the malicious code will attempt to find and infect other computers. This code can also propagate via email, websites, or network-based software.
  - Some malicious code claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

  Viruses and worms are examples of malicious code.
- Vulnerability - In most cases, vulnerabilities are caused by programming errors in software. Attackers might be able to take advantage of these errors to infect your computer, so it is important to apply updates or patches that address known vulnerabilities (see Understanding Patches for more information).

This series of cyber security tips will give you more information about how to recognize and protect yourself from attacks.

TLP:WHITE

References

TLP:WHITE

- Understanding patches
- The Comprehensive Cyber Security Initiative

Authors

Mindi McDowell and Allen Householder

TLP:WHITE