How Does Cybersecurity Matter to Me?

Air Force Association

Understanding the Risks and Preventing Harm

Using the Internet has become an integral part of life in the modern world. From communicating via email and instant message to reading the news and shopping, nearly every aspect of our life revolves around the cyber world. Because the Internet is so widely used, protecting vital information in the cyber world is not only our responsibility, but a necessity to preserve our national security.

How am I at Risk?

Unauthorized users that invade a system are commonly known as hackers, and hackers have a wide variety of tools to harm a computer system. Hackers usually gain access to systems by planting malicious logic (like a virus) somewhere on the net and waiting for users to encounter or open the virus. Common ways a computer can become infected are:

- Opening an email attachment that contains malicious logic
- Visiting a malicious website
- Clicking on a dangerous link
- Inadvertently downloading a harmful program

What kind of damage can a hacker do?

Infected computer systems may be affected and damaged in a variety of ways, sometimes without a user even noticing. Some hackers are "playing a prank," while others may be attempting to steal personal information such as credit card numbers, Social Security numbers, or other personal information. Even worse, hackers can take control of an infected computer and use it to launch an attack on a larger system. Even if your computer has no stored sensitive data, it can still be used to infect other computers without your knowledge! This practice is so prevalent that access to vulnerable or infected computers is bought and sold among hackers.

How can I protect myself?

Most hackers use malicious logic to exploit vulnerabilities in software and gain unauthorized access to computer systems. For this reason, it is vitally important to install and update anti-virus and firewall software. Because new vulnerabilities in computer systems are found every day, computer companies "patch" these vulnerabilities by issuing a series of system updates. To ensure your computer is safe from known vulnerabilities, make sure to install all updates on a regular basis. Some other basic security measures include:

- Creating a strong password that has at least nine characters, contains a capital letter, uses a special character (such as #,!,%,*) and includes a number.
- Consistently tracking your credit information so that if your computer is infected, you can minimize damage
- Backing up important information on your computer

Only visit websites you trust, and open emails only from known contacts.