VAStar Cyber Security

Introduction to Cyber Security

Goals

- Define 'Cyber Security'
- Learn about the ethical use of computers
- Read about recent hacking attacks. Identify the victim, the attacker, the motive, and the result.
- Read examples of Cyber Security threats and determine if the people acted ethically
- Identify some methods hackers use to gain access to a computer network

What is Cyber Security?

Cyber security is the protection of computer systems from the theft and damage to their hardware, software, or information, as well as from disruption or misdirection of the services they provide.

Any person who is actively working to protect a computer from damage or protect digital data from being stolen is performing cyber security.

Typically, practicing cyber security is necessary to protect systems which are targeted by groups acting unethically.

What is ethical computing?

Ethical computing is a philosophy that teaches how computing professionals should make decisions regarding professional and social conduct. The Computer Ethics Institute (CEI) in Washington, D.C. is a nonprofit organization tasked with advancing the teachings of ethical computing.

The CEI wrote a short code of ethics titled the "Ten Commandments of Computer Ethics" in 1992, which describe how they feel computers should be ethically used.

The Ten Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid (without permission).
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Is Cyber Security needed?

Unfortunately, unethical computing is happening all around us. Cyber security is needed to keep important systems and data safe, especially when the stakes are high, such as in government, healthcare, financial institutions, manufacturing, and transportation.

Governments and companies are spending more money and resources than ever in the cyber security space to protect mission critical services and data. 2017 has seen some of the most devastating cyber attacks ever, showing no signs of slowing down.

Recent hacking events

Research the following hacking events online and try to determine the victim, the attacker, the motive, and the result. How could these attacks been avoided? Feel free to discuss these attacks with your peers.

- NSA software stolen by Shadow Brokers, 2017
- WannaCry ransomware, 2017
- Deep Root Analytics US voter record breach, 2017
- Equifax credit reporting breach, 2017
- Yahoo user account breach, 2016
- Playstation Network and Xbox Live Christmas hack, 2014
- Mt Gox bitcoin exchange hack, 2011

How do hackers gain access to systems?

Hackers don't usually type quickly on multiple screens to gain access to systems as seen on TV. Although software exploits are one of the ways hackers operate, there are many more ways that hackers can manipulate systems and people to gain unauthorized access to computers and data.

- Software Exploits - abusing bugs or flaws in software to gain access
- Physical Access - accessing the device in person
- Social Engineering - tricking people with access to perform an action or give access
- Malware - using computer software to steal data or gain access
- Stolen or guessed passwords - using the credentials of those who have access