Cybersecurity Education

What is Cybersecurity?

- Cybersecurity standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cybersecurity attacks.
- Cybersecurity refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.
- Cybersecurity is important for network, data and application security.
- Communication security is protection organization communication media, technology and content.
- Network security is the protection of networking components, connection and content.
- Information security is the protection of information and its critical elements, including the systems and hardware that use, store or transmit that information.

What is Cybercrime?

The former descriptions were “computer crime”, “computer-related crime” or “crime by computer”. With the pervasion of digital technology, some new terms like “high-technology” or “information-age” crime were added in the definition. Also the Internet brought other new terms, like “cybercrime” and “net” crime.

Other forms include “digital”, “electronic”, “virtual”, “IT”, “high-tech” and “technology-enabled” crime.

History

- The first recorded cyber-crime was in the year 1820.
- The first spam email took place in 1978 when it sent over the ARPAnet.
- First Virus: While the technical definitions for computer virus, worm, and malware might have a little overlap, it’s generally accepted that the first type of computer “virus” occurred in 1971 on ARPAnet, the scientific/military network that preceded the modern internet. Creeper was an experimental self-replicating program that infected DEC computers across the network — this would be considered a computer worm today.

How to Protect your Computer

- Keep your Firewall turned on.
- Install or update your Antivirus Software.
- Install or update your Antispyware Technology.
- Keep your Operating System up to date.
- Be careful what you download.
- Turn off your computer.
- Check security settings.
- Use secure connection.
- Open attachments carefully.
- Use strong passwords.
- Do not give personal information unless required.
- Use antivirus software.
- Insert firewalls, pop up blocker.
- Uninstall un-necessary software.
- Maintain backup.

Responding to an Incident

- Access the nature and scope of an incident and identify what information systems have been misused.
- Take appropriate steps to contain and control the incident to prevent further misuse.
- Notify your financial institution of an unauthorized access.