Cybersecurity

AL Mansour University College

Digital Media Department

4th Class

Lecturer Mustafa Muhanad

-2-

1.4. Cyber Security and Information Security

The terms Cybersecurity and Information Security are often used interchangeably. As they both are responsible for the security and protecting the computer system from threats and information breaches and often Cybersecurity and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously.

Information security can be simply defined as “a set of strategies for managing the processes, tools, and policies necessary to prevent, detect, document and counter threats to digital and non-digital information.” Any point of data storage and transfer is considered to be an “information system,” meaning this practice can apply to a wide variety of environments, including that outside cyberspace. Data security is all about securing data. Now another question that arises here is the difference between data and information? Not every piece of data can be information. Data can be called information when it is interpreted in a context and given meaning. For example, “14041989″ is data. And if we know that this is the date of birth of a person, then it is information. So, Information means data that has some meaning.

Information security is all about protecting the information, which generally focuses on the confidentiality, integrity, availability (CIA) of the information. While cybersecurity is about securing things that are vulnerable, it also considers that where data is stored and technologies used to secure the data. Part of cybersecurity about the protection hardware and software, is known as information and communications technologies (ICT).

Difference between Cybersecurity and information Security

Cybersecurity	Information Security
It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal to provide confidentiality, integrity, and availability.
It is about the ability to protect the use of cyberspace from cyber-attacks. Cybersecurity to protect anything in the cyber realm. Thus, it deals with danger against cyberspace.	Information security is for information irrespective of the realm. Thus , Its deals with the protection of data from any form of threat.
Cybersecurity strikes against Cybercrimes, cyber frauds , and law enforcement.	Information security strives against unauthorized access, disclosure modification, and disruption
On the other hand cybersecurity professionals deal with the advanced persistent threat.	Information security professionals are the foundation of data security and security professionals associated with it prioritize resources first before dealing with threats.

1. 5. Computer and Internet Safety

For Computer and Internet Safety it's better to understand security threats associated with the use of computers and the internet, and by understanding how these threats are exploited, we can better protect our congregation, our congregation's information, computers, and computer files.

The following tips are considered the most common tips needed for Computer and Internet Safety:-

1) Run antivirus software and keep all computer software patched

2) Use a unique, strong password to access resources and every site/service you use, opt-in for multifactor authentication.

3) Learn to identify phishing emails and social engineering and use email securely

4) Work as a non-administrator on your computer

5) Use secure Wi-Fi and practice network security.

6) Back up important information.

7) Secure your mobile device.

8) Limit social network information.

9) Download files legally.

1. 6. Internet Governance – Challenges and Constraints

To understand Internet governance challenges, it is important to have a clear idea of the main technical principles. “ The Internet is a communication network made up of millions of networks, owned and operated by various stakeholders . It connects these networks to each other and facilitates the overall exchange of information. Hundreds of stakeholders have been involved in the design and regulation of the Internet, including governments, international organizations, companies, and technical committees among many others".

“Internet governance is the development and application by Governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet".

The following are the most Internet Governance Challenges and Constraints :

• Many issues, many institutions

• Rapid technological progress

• Rapid societal impact

• Need structure, abstraction, models, and taxonomies.

There are some structural similarities between the governance problems in cybersecurity and internet governance. Since both are used to make internet services, they are heavily dependent on each other. Because of this, the models used for cybersecurity governance and internet governance need to work together, and how we handle one will affect how we handle the other.