Data Security

Security Concepts

Kassem Danach, Eng., PhD

LEARNING OBJECTIVES

1. Data Threats
   a. Distinguish between data & information, understand the terms cybercrime & hacking.
   b. Recognize data threats from individuals, external organizations, and force majeure.
2. Value of Information
   a. Understand the reasons for protecting personal and workplace information.
   b. Basic characteristics of Information Security.

LEARNING OBJECTIVES

3. Personal Security
   a. What is social engineering? Identify methods of social engineering.
   b. Understand the term identity theft and its methods.
4. File Security
   a. Setting passwords for documents and files.

DATA THREATS

- Although technology is supposed to make life easier in many ways, it is unfortunate that people also use technology to take advantage of others.
- A threat can be anything from a virus attack, stealing information, to an “act of God” such as a fire, flood and earthquakes.

DIFFERENCE BETWEEN DATA AND INFORMATION

- **Data** is raw, unprocessed information. Data can be simple, random and useless until processed.
- Once data is processed, organized, structured & presented or communicated it becomes **information.**

CYBERCRIME

- is any type of illegal activity using a computer, the Internet, a private or public network.
- Including monetary and non-monetary offenses.

HACKING, CRACKING, ETHICAL HACKING

- **Hacking** is the use of computer and network resources to get unauthorized access to information, and not do any harm.
- **Cracking** is taking hacking one-step further. Once the system is hacked, the purpose is to cause harm.
- Many companies employ hackers to help them identify potential threats to their systems or network, this is called **Ethical Hacking**.

RECOGNIZE THREATS TO DATA

- **Force Majeure,** refers to disasters caused by natural forces that cannot be controlled by humans.
- **Insider Threats** meaning that businesses are at risk by actions from those on the inside, Including:
  - **Employees**
  - **Service Providers**
  - **External Insiders**

VALUE OF INFORMATION

- **PROTECTING PERSONAL INFORMATION**
  - **Identity theft** means stealing information (name, address, telephone number, date of birth) and using it without ones permission in order to commit fraud.
- **PROTECTING COMMERCIAL INFORMATION**
  - A company must keep client information safe.

MEASURED FOR PREVENTING UNAUTHORIZED ACCESS TO DATA

- **Username –** A unique name used to identify who is attempting to log onto a computer or network.
- **Password –** A sequence of characters used to determine that a user requesting access to a system is really that particular user.
- **Encryption** – is the translation of data into a secret code.

BASIC CHARACTERISTICS OF INFORMATION SECURITY

- **Confidentiality –** confidentiality of information ensures that only those with privileges may have access.
- **Integrity –** is the quality or state of being whole, complete and uncorrupted.
- **Availability –** ensures reliable and timely access to data and resources by authorized people.

SOCIAL ENGINEERING

- Social engineering is the art of manipulating people to give up personal and confidential information.

SOCIAL ENGINEERING

- **Methods of Social Engineering**
  - Phone Calls (Vishing)
  - Phishing
  - Shoulder Surfing

IDENTITY THEFT

- Identity Theft means obtaining personal or financial information of another person for the sole purpose of using that person or business name for fraudulent purposes.

IDENTITY THEFT

- **Methods of Identity (ID) Theft**
  - Information Diving
    - Dumpster Diving
    - Mail Theft
    - Social Media
  - Skimming
  - Pretexting

File Security

- **Set Passwords For Files**
  - Passwords can be set to protect different kinds of documents or files, such as Word processing, PowerPoints, and compressed files.
  - Not all files need to protection, however it might good to password protect files containing sensitive information.