**Digital Security**

#### **Cyber Security** is a set of methods for protecting computer systems from cyber attacks.

Here are instructions on how to create a strong password that you can rely on:

1. **Never use personal information**: Strong passwords shouldn’t include references to any personal information.
2. **Use a combination of letters, numbers, and symbols**: Secure passwords include random characters, numbers, and letters. Passwords also must be as long as possible.
3. **Never repeat passwords:** Reusing the same password for different accounts puts you at risk of getting all accounts hacked after a single data leak.
4. **Avoid using real words**: Hackers use malicious programs that can process every word found in a dictionary to crack passwords. Stay away from using proper nouns and other dictionary words that could lead to an unsecure password.

**Hardware security** is vulnerability protection that comes in the form of a physical device rather than software. Hardware security can pertain to a device used to scan a system or monitor network traffic. Common examples include hardware firewalls and proxy servers. Hardware security is defined as the protection of physical devices from threats that would give unauthorized access to enterprise systems.

**Malware** is intrusive software that is designed to damage and destroy computers and computer systems. **Types of** **malware: Virus, Worms, Trojan virus, Spyware, Adware, Ransomware and Fileless malware.**

**Social engineering** is the art of manipulating people so they reveal confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

**Encryption** is commonly used to protect data stored on computer systems and data transmitted via computer networks, including the Internet. Financial transactions and private messaging communications often use encryption to increase security. For data communicated over a network, modern encryption scrambles data using a secret value or key known only by the recipient and the sender. For stored data, the secret value is typically known only by the data owner.