Cybersecurity — Digital Safety & Encryption

Title: Principles of Cybersecurity: Encryption and Digital Safety

Cybersecurity is the practice of protecting computer systems, networks, devices, and data from theft, damage, disruption, or unauthorized access. A foundational concept in cybersecurity is the **CIA Triad**, which outlines the three core goals of information security:

1. **Confidentiality:** Ensuring that data is accessible only to authorized individuals.
2. **Integrity:** Maintaining the accuracy and completeness of data, ensuring it is not altered or tampered with.
3. **Availability:** Ensuring that systems and data are operational and accessible to authorized users when needed.

Encryption is the primary technology used to ensure **Confidentiality**. It is the process of converting readable data (plaintext) into an unreadable, scrambled format (ciphertext) using a mathematical algorithm and a secret "key." Only someone with the correct key can decrypt the ciphertext back into its original plaintext form.

There are two main types of encryption:

- **Symmetric Encryption:** This method uses a single, shared secret key to both encrypt and decrypt data. It is very fast and efficient, making it ideal for encrypting large amounts of data, such as the files on your hard drive. The Advanced Encryption Standard (AES) is the most common symmetric algorithm. The main challenge is securely sharing the secret key with the intended recipient.
- **Asymmetric Encryption (Public-Key Cryptography):** This method uses a pair of keys: a **public key** and a **private key**. The public key can be shared with anyone and is used to *encrypt* data. The private key is kept secret by the owner and is the only key that can *decrypt* the data. This system, (e.g., RSA algorithm), is the backbone of secure internet communication, such as HTTPS (the "lock" icon in your browser) and secure email.

Digital Safety refers to the personal practices and habits that protect an individual's digital identity and assets. While encryption protects data in transit, digital safety practices protect you from attacks that target human behavior. Key practices include:

- **Strong, Unique Passwords:** Avoiding common or reused passwords. Using a **password manager** is the best way to create and store complex, unique passwords for every account.
- **Multi-Factor Authentication (MFA):** This provides a critical layer of security by requiring a second form of verification (like a code from your phone) in addition to your password.
- **Phishing Awareness:** Being suspicious of unsolicited emails, texts, or messages that create a sense of urgency and ask for personal information or login credentials.
- **Software Updates:** Regularly updating your operating system, browser, and applications to patch security vulnerabilities that hackers could exploit.