# Beginner’s Guide to Cybersecurity

## What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks. It involves implementing measures to defend against cyber threats, such as hackers, malware, and phishing attacks. With the increasing reliance on digital technology, cybersecurity has become essential for individuals and businesses alike.

## Types of Cyber Threats

### 1. Malware

Malware (malicious software) includes viruses, worms, trojans, and ransomware that can damage or disrupt systems.

### 2. Phishing

Phishing attacks trick users into revealing sensitive information, like passwords, through fake emails or websites.

### 3. Hacking

Hacking refers to unauthorized access to computer systems to steal, alter, or destroy data.

### 4. Social Engineering

Social engineering manipulates people into divulging confidential information through deception.

## Basic Cybersecurity Practices

### 1. Use Strong Passwords

Create strong passwords using a mix of letters, numbers, and symbols. Avoid using common words or personal information.

### 2. Enable Two-Factor Authentication (2FA)

Adding an extra layer of security with 2FA helps protect accounts from unauthorized access.

### 3. Keep Software Updated

Regularly updating software ensures you have the latest security patches against vulnerabilities.

### 4. Be Cautious with Emails and Links

Avoid clicking on suspicious links or attachments in emails to prevent phishing and malware infections.

## Protecting Personal Devices & Data

To stay safe online, always use antivirus software, back up your data regularly, and avoid connecting to unsecured public Wi-Fi networks. Using a VPN (Virtual Private Network) can also enhance online privacy and security.