# Hacking and Cybersecurity

Cybersecurity is the practice of protecting computers, networks, and data from attacks or unauthorized access. Hacking means trying to get into systems or networks — sometimes for bad reasons, and sometimes to test security (ethical hacking).

## Common Types of Cyber Attacks

• Phishing: Fake messages or websites that trick people into giving personal information (like passwords).

• Malware: Harmful software that can steal data or damage a computer.

• DDoS (Denial of Service): Sending too many requests to a website so it stops working.

• Exploits: Using software bugs or system weaknesses to break in.

• Brute Force Attack: Trying many passwords until one works.

## Examples

• You get an email saying 'Click here to win a prize' → fake website → steals your password → Phishing.

• You open a strange file → your computer slows down → Malware.

• A website becomes very slow because too many people (or bots) visit at once → DDoS.

## Basic Cybersecurity Rules

• Always update your software and system.

• Use strong and different passwords for each account.

• Turn on two-factor authentication (2FA).

• Don’t open links or attachments from unknown senders.

• Make regular backups of your important files.

• Use antivirus software and scan your device often.

• Give apps and people only the permissions they really need.

## Types of Hackers

• Black Hat: Hackers who break into systems for bad or illegal reasons.

• White Hat: Ethical hackers who test systems to improve security.

• Grey Hat: In between — they may hack without permission but not for bad goals.

## Tips for Everyday Safety

1. Turn on two-factor authentication on all your accounts.

2. Don’t reuse the same password.

3. Be careful with emails or messages that ask for personal info.

## Conclusion

Cybersecurity helps protect our digital life. Hacking can be dangerous, but with awareness and simple safety steps, anyone can stay safe online.