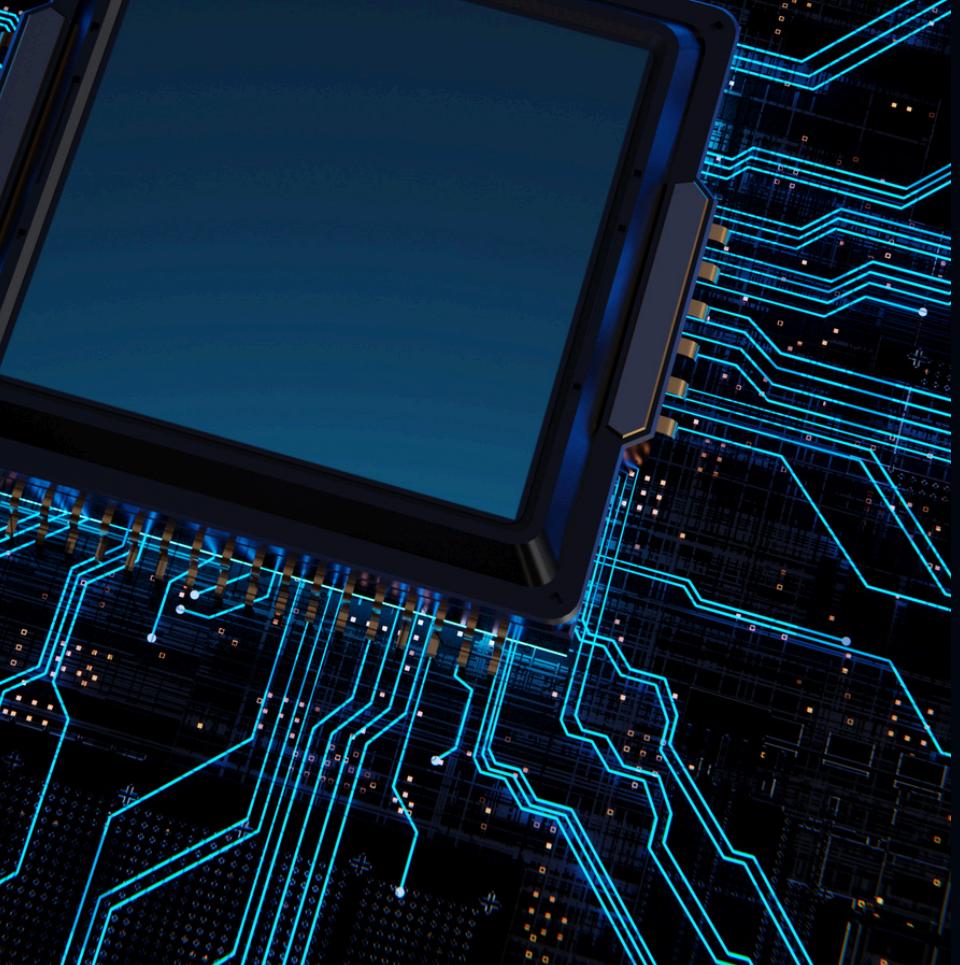




# CYBER SECURITY





# INTRODUCTION

- ◆ Cyber threats are increasing, affecting individuals and businesses.
- ◆ Malicious software (malware) is designed to harm or exploit systems.

Evolution of Attack

90%



# WHAT IS MALICIOUS SOFTWARE?

Malicious software (malware) is any program designed to damage, steal, or exploit data.

## HOW IT SPREADS:

✓ EMAIL ATTACHMENTS

✓ FAKE SOFTWARE DOWNLOADS

✓ INFECTED WEBSITES

✓ USB DEVICES

# TYPES OF MALWARE

- 
- ```
graph TD; A[TYPES OF MALWARE] --- B[1 Virus]; A --- C[2 Worms]; A --- D[3 Trojan Horse]; A --- E[4 Ransomware]; A --- F[5 Spyware]; A --- G[6 Keyloggers]; A --- H[7 Botnets]
```
- 1 Virus - Attaches to files and spreads when executed.
  - 2 Worms - Self-replicating malware that spreads without user action.
  - 3 Trojan Horse - Disguises itself as legitimate software.
  - 4 Ransomware - Encrypts files and demands payment to unlock them.
  - 5 Spyware - Secretly monitors user activity.
  - 6 Keyloggers - Records keystrokes to steal passwords.
  - 7 Botnets - A network of infected devices controlled remotely.



# Live Demonstration

- ◆ A hacker creates a fake login page that looks like a real website.
- ◆ The victim unknowingly enters their username and password.
- ◆ The hacker steals the credentials and gains access to the victim's account.



# PREVENTION AND HOW TO AVOID

- ✓ Check URLs before entering login credentials.
- ✓ Avoid clicking on unknown email links.
- ✓ Enable Two-Factor Authentication (2FA).
- ✓ Verify emails from banks or organizations.
- ✓ Use anti-phishing browser extensions.

