ANATOMY OF A CYBER ATTACK

1 PRE-ATTACK PHASE

Reconnaissance
Researching the target, including network structure and employee details.

Vulnerability Scanning
Identifying weaknesses in systems and software.

Weaponization
Creating or acquiring malicious payloads to exploit vulnerabilities.

2 ATTACK PHASE

Initial Compromise
- **Delivery |** Malicious payload is delivered via email, websites, or attachments.
- **Exploitation |** Payload executes to gain unauthorized access.

Installation
Installing malware like backdoors or ransomware.

Command and Control (C2)
Establishing communication with the compromised system.

Lateral Movement
Moving through the network to compromise additional systems.

Privilege Escalation
Gaining higher access levels for full control.

3 POST-ATTACK PHASE

Data Exfiltration
Stealing sensitive information and transferring it out.

Impact and Damage
Disruption, downtime, and reputational damage.

Cover-Up
Deleting logs and hiding traces of the attack.

Post-Attack Analysis
Detecting the breach, investigating, and beginning remediation.

4 MITIGATION & PREVENTION

Security Awareness Training
Educating employees on cybersecurity threats and practices.

Regular Updates and Patching
Keeping systems and software up to date.

Network Segmentation
Isolating critical systems to limit attack spread.

Incident Response Planning
Developing and practicing a response plan for breaches.

LEARNING TREE™ INTERNATIONAL