

# Introduction

- ▶ A network attack can be defined as any method, process, or means used to maliciously attempt to compromise network security.





# Types Of Network Attack

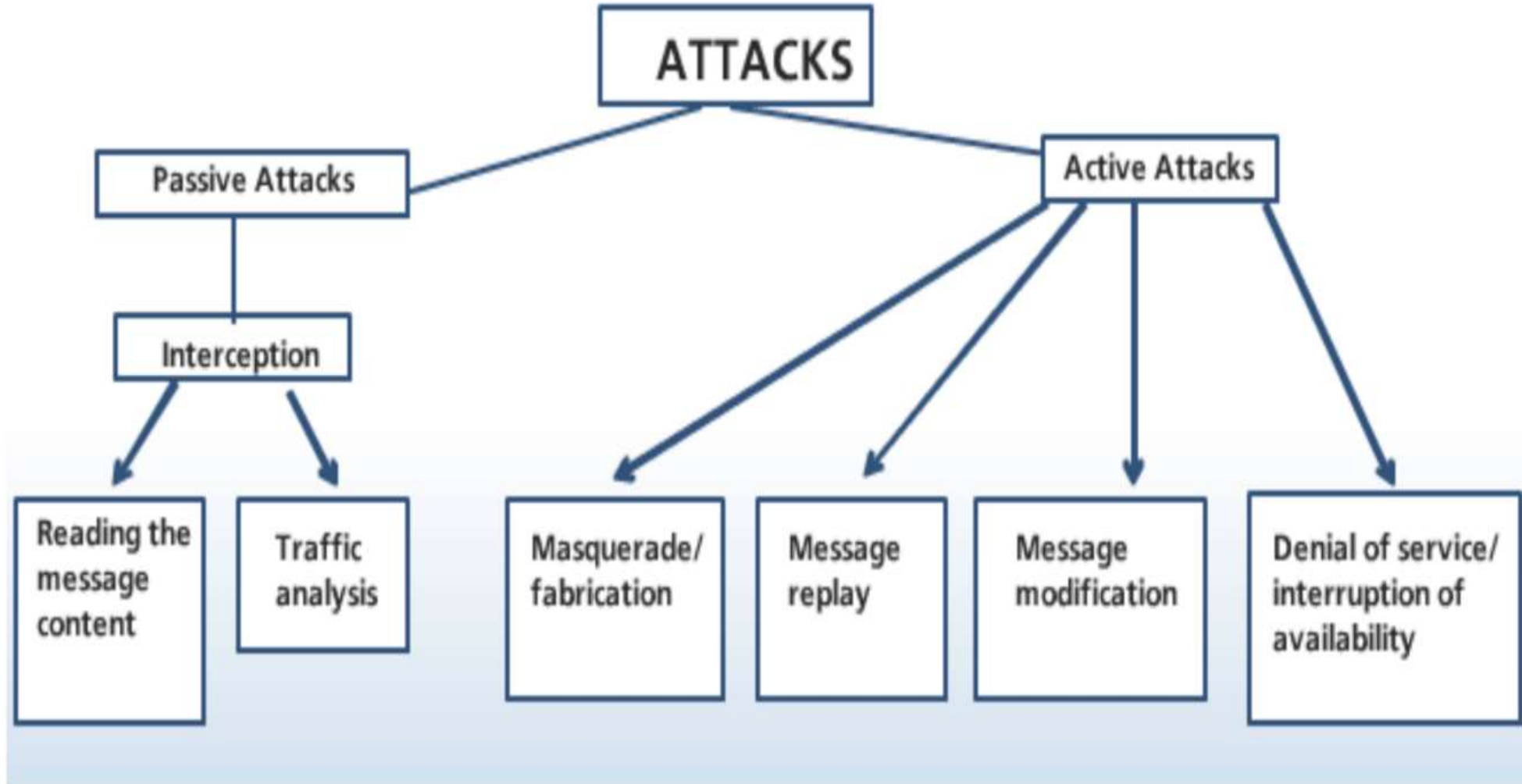


ACTIVE ATTACK



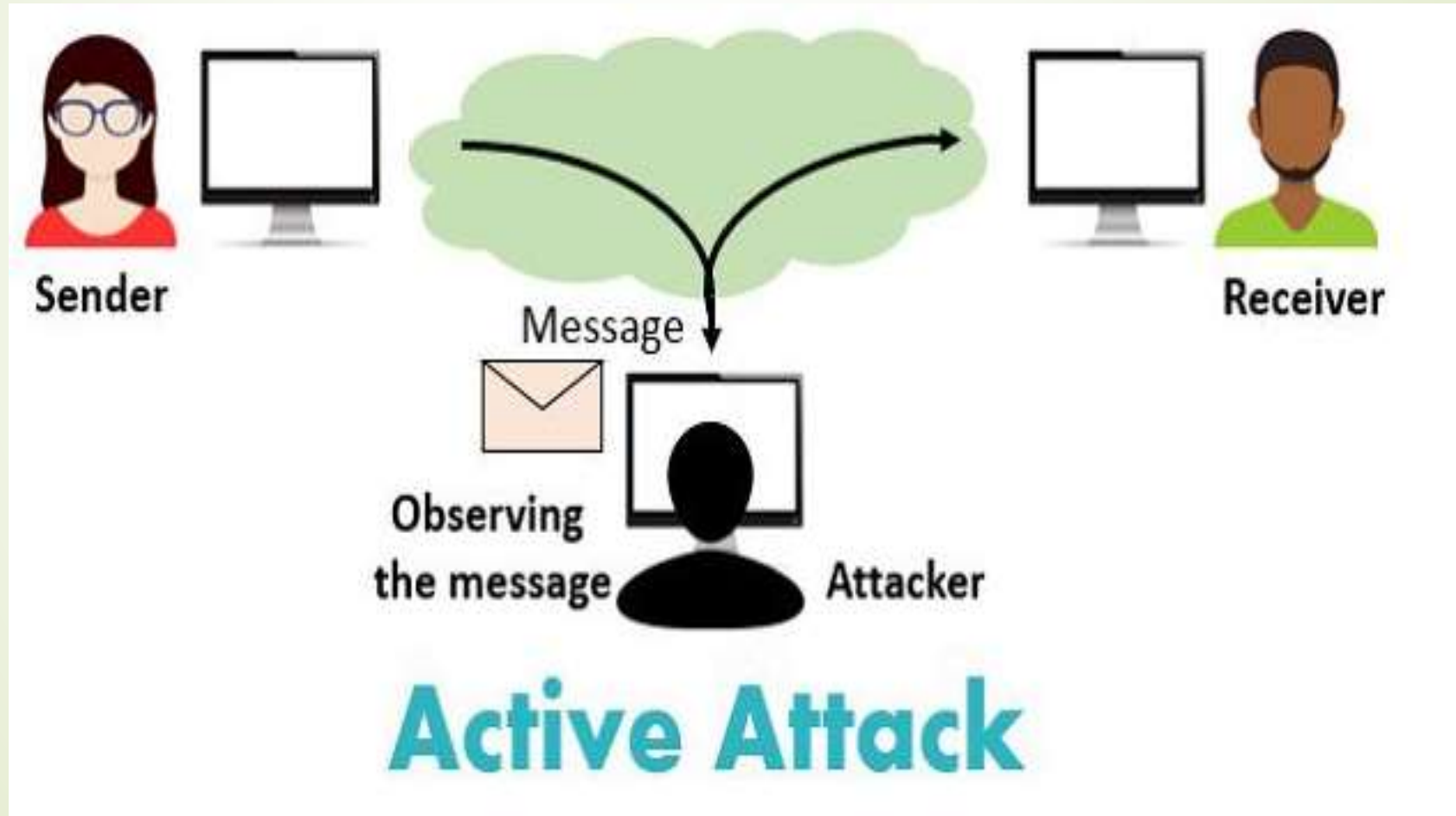
PASSIVE ATTACK

# Active Attack and Passive Attack



# Active Attack

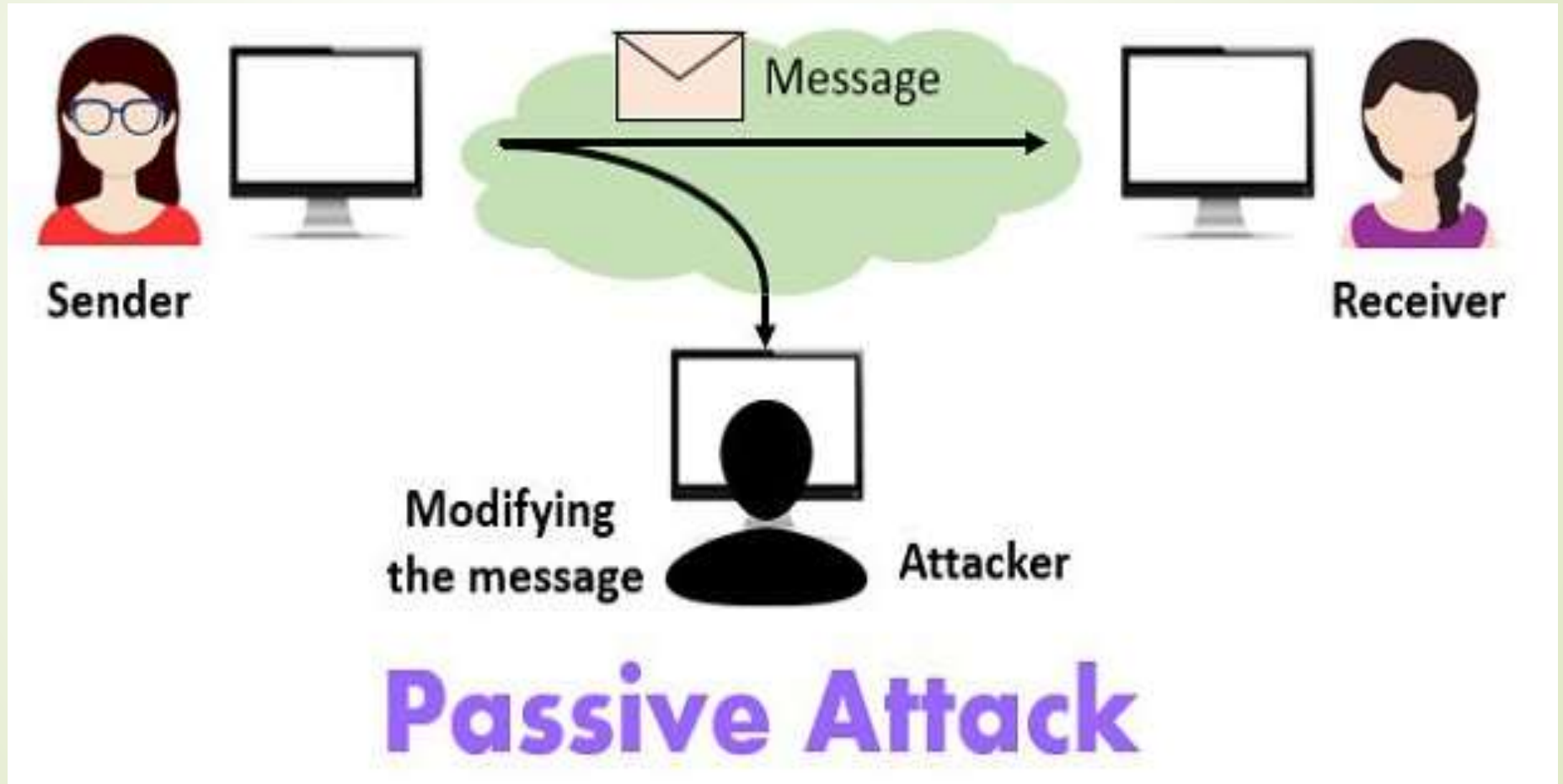
- Active attack tries to change the system resources or affect their operation. Always causes damage to the system.





# Passive Attack

Passive attack tries to read or make use of information from the system but does not influence system resources.





# Basic Network Attack

- Password Based Attack
- Malware Attack
- DOS Attack
- IP Spoofing
- Man in the Middle Attack
- SQL injection Attack
- XSS Attack

# Password Based Attack

- An attack in which repetitive attempts are made to duplicate a valid logon or password sequence.



# Malware Attack

**Norton Security** Sign In

Settings | Help | Search

## You Have Been Hacked!

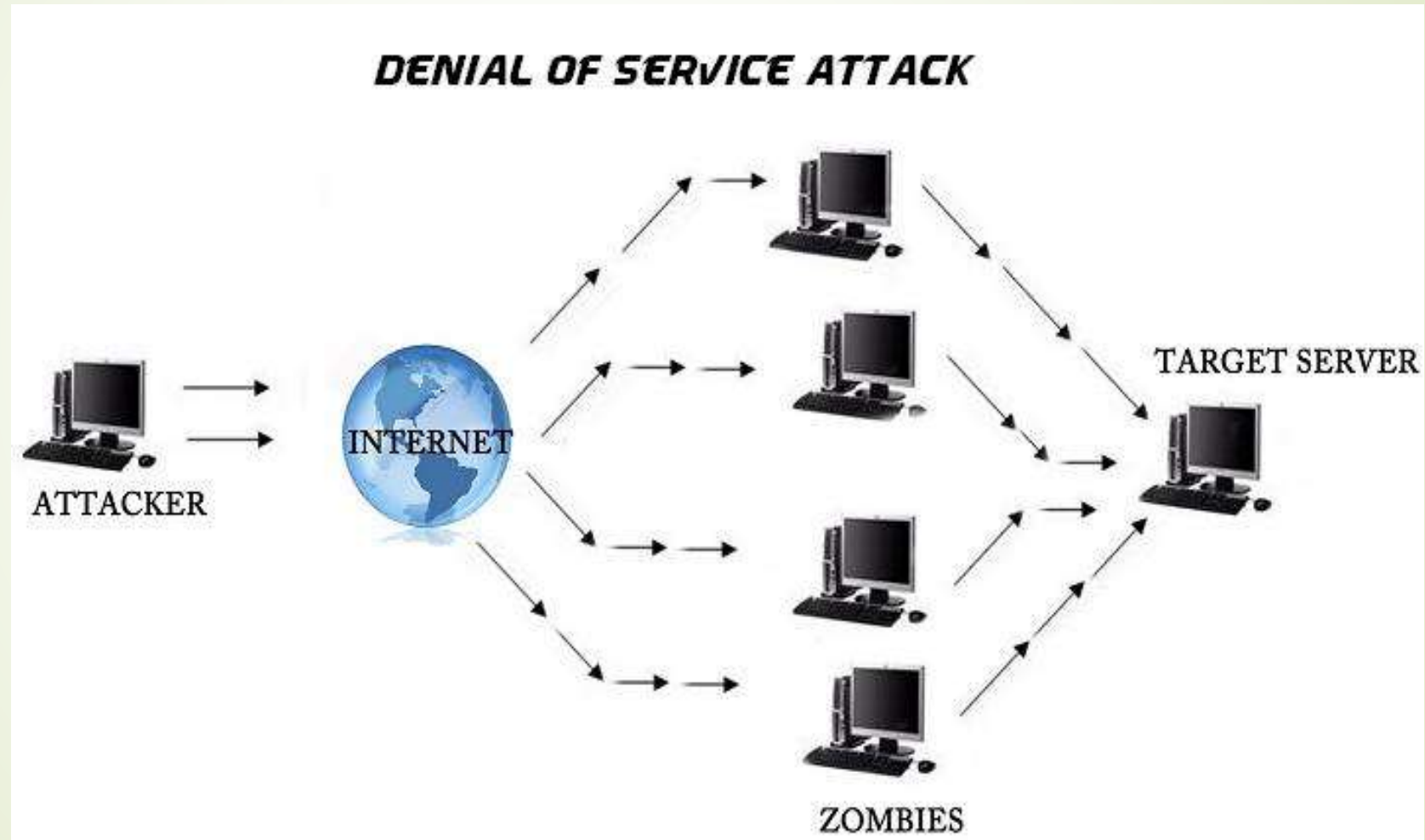
Your computer, network and web protections are at risk.

Malware	Ransomware	Spyware	Destruction
Infesting Computer...	Encrypting Files...	Stealing Data...	Destroying Data...

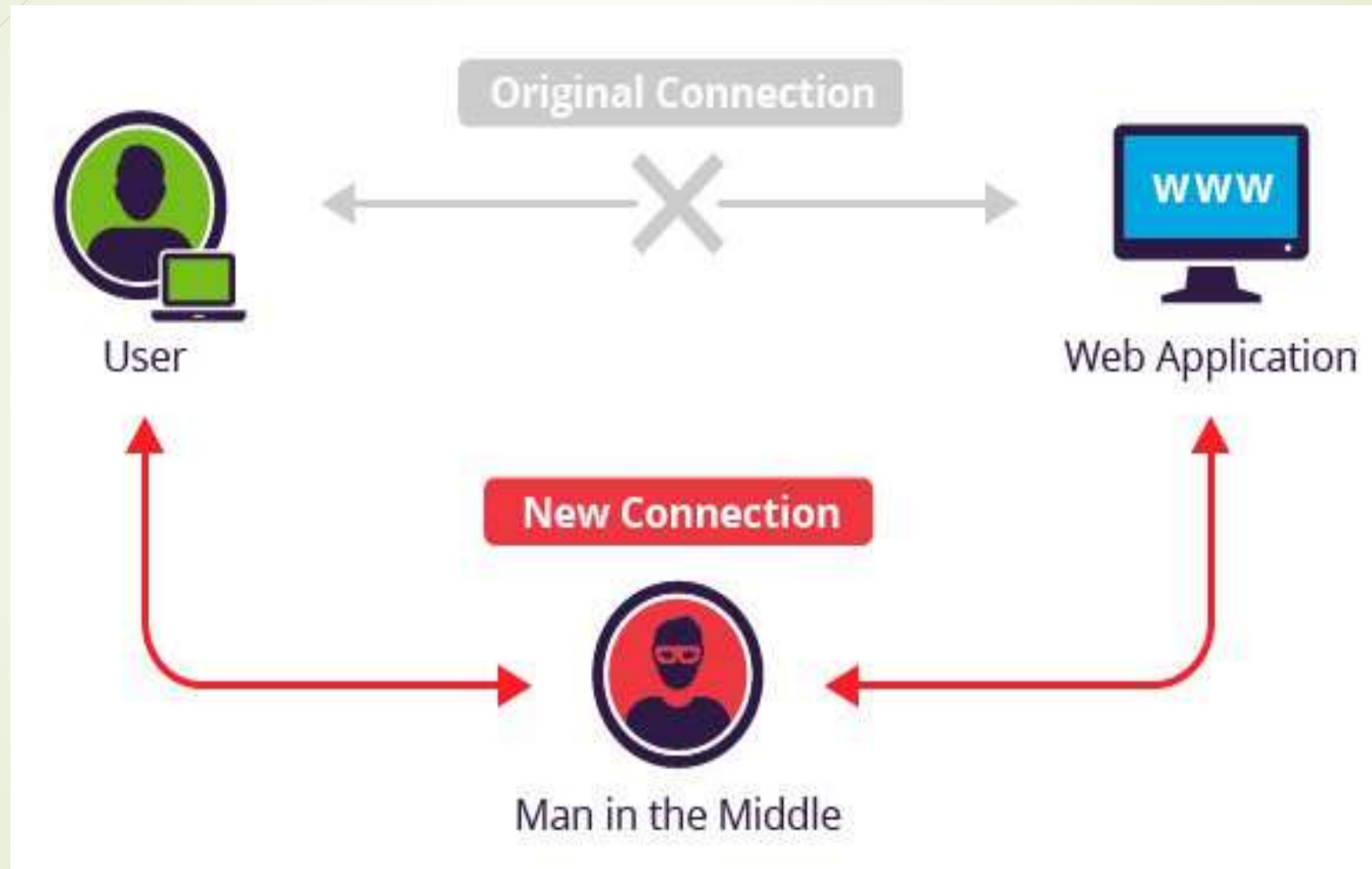
SUBSCRIPTION STATUS: 30 Days Remaining | [Subscribe](#)



# DOS ATTACK

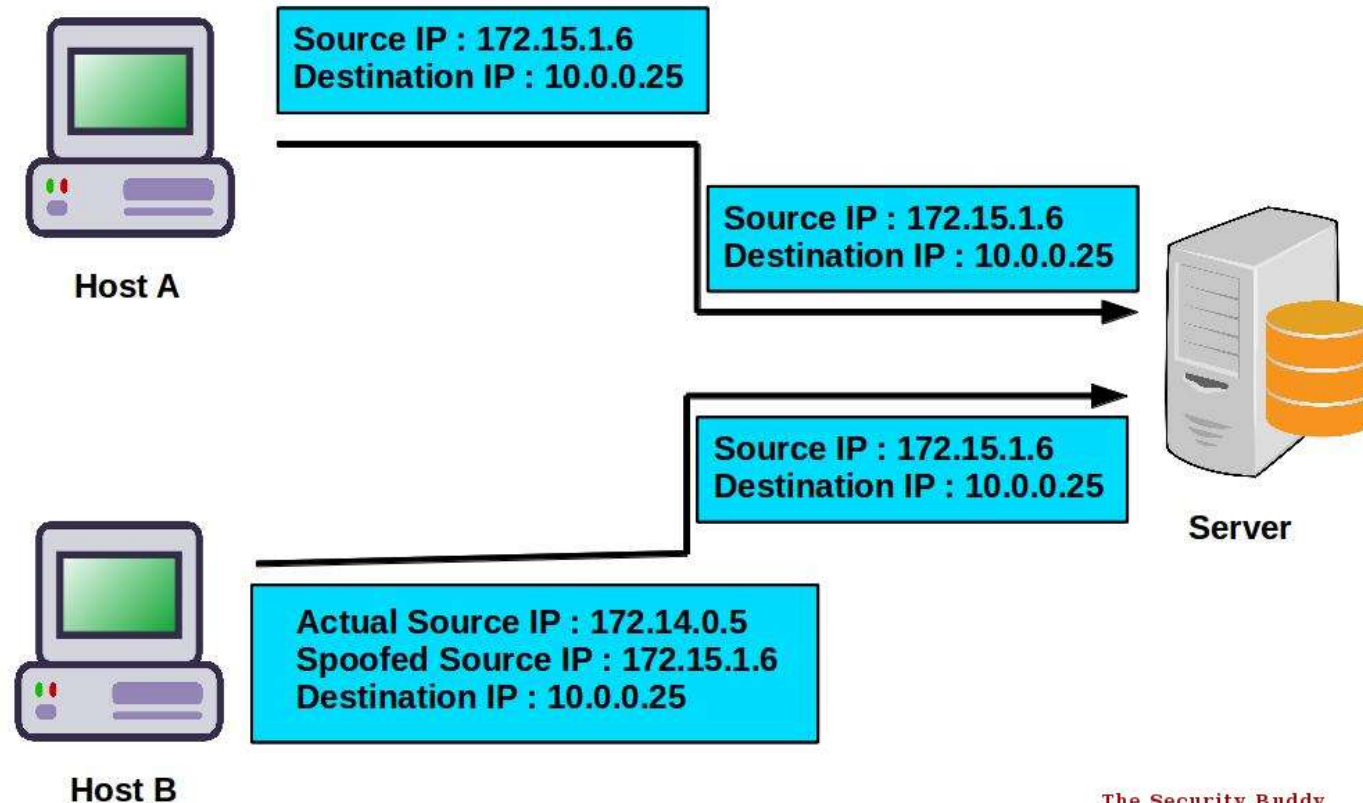


# MAN IN THE MIDDLE ATTACK



# IP SPOOFING

## IP Address Spoofing



# SQL INJECTION ATTACK

## WHAT IS SQL INJECTION?



A SQL query is one way an application talks to the database.

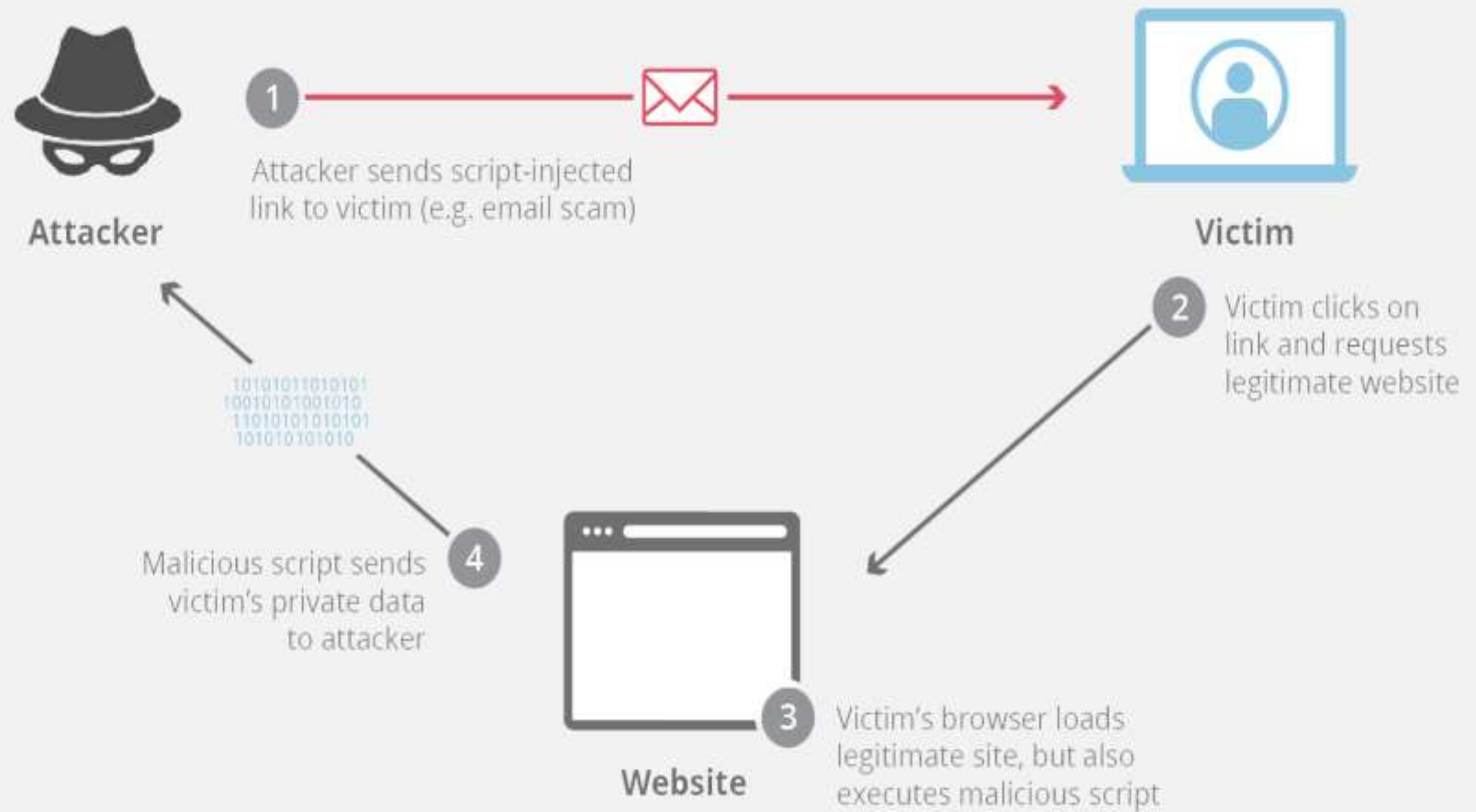


SQL injection occurs when an application fails to sanitize untrusted data (such as data in web form fields) in a database query.



An attacker can use specially-crafted SQL commands to trick the application into asking the database to execute unexpected commands.

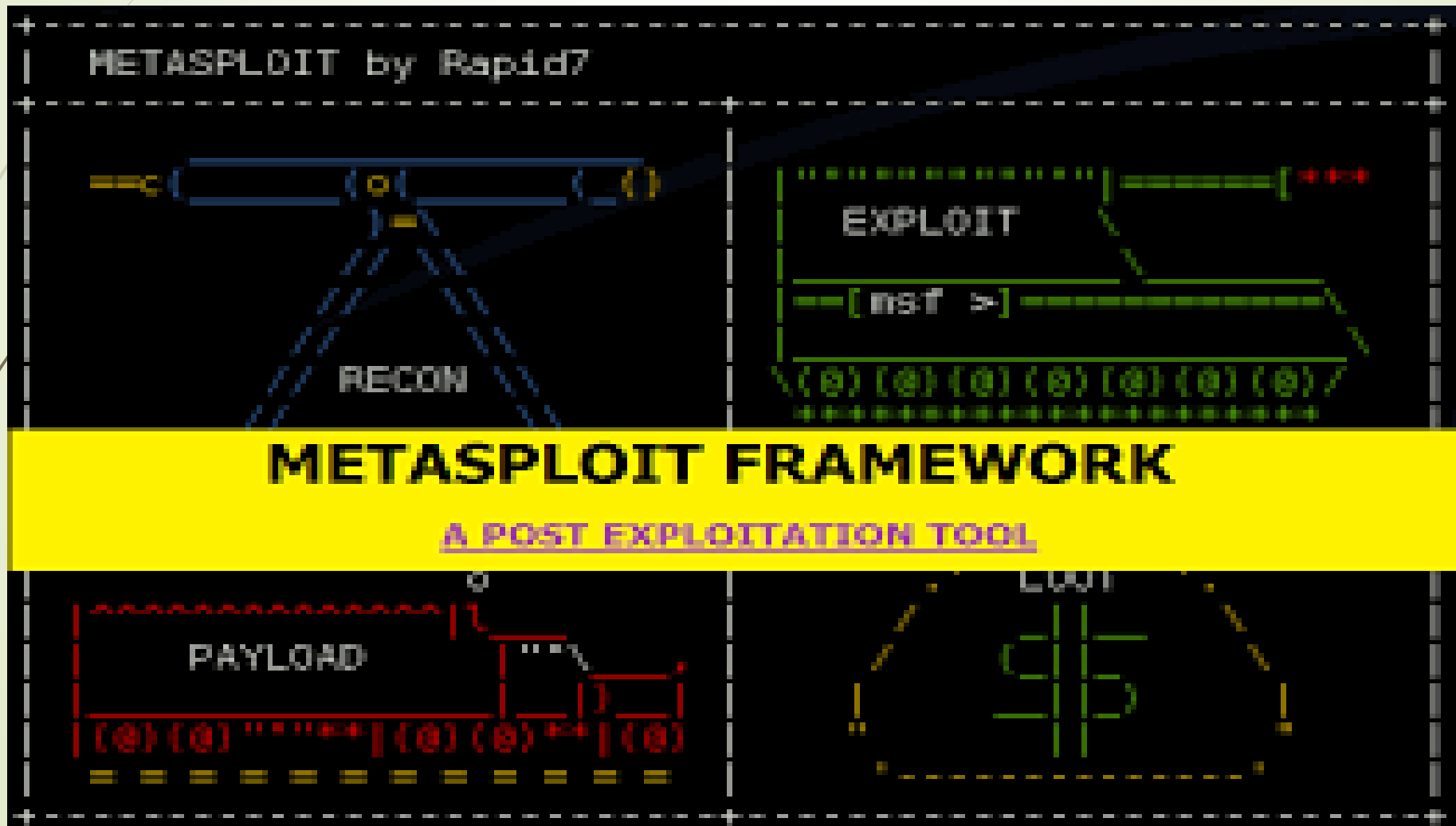
# XSS ATTACK





# Network Attackers Tool(Penetration Testing Tool)

## Metasploit Framework





- Ettercap

- sqlmap

- Kali Linux

- Social Engineering Tool Kit

- Cain and Able



# Network Attack Prevention Tips

- Install Software Updates
- Use Unique Password
- Use Two Factor AUTHENTICATION
- USE STRONG PASSSSWORD
- USE A PASSWORD MANAGER
- Use a firewall for your Internet connection.
- Browse Safely Online
- Clear Browser after Leaving Computer