

THE UNIVERSE OF CYBER THREATS

MALWARE

Malware, short for "malicious software", is designed to infiltrate & harm computers, mobiles devices and networks.

It can be introduced through methods like viruses, trojans & ransomware.

RANSOMWARE

TROJAN

VIRUS

ZERO - DAY EXPLOIT

A zero-day exploit refers to a cyber attack that exploits a software vulnerability that is not yet known to the software vendor or antivirus providers. The attacker spots the software vulnerability before any parties interested in mitigating it, quickly creates an exploit, and uses it for an attack.

DISTRIBUTED DENIAL OF SERVICE ATTACKS

A DDoS attack is a type of cyber attack where multiple compromised systems collaborate to disrupt an online service, server or network by flooding the target with harmful traffic, causing to become unavailable.

PHISHING

Phishing is a form of fraud that tricks individuals into sharing sensitive data such as usernames, passwords and banking information. The goal is to manipulate people into disclosing their confidential details.

VISHING

SMISHING

IP spoofing

Email hijacking

INSIDER THREATS

Insider Threats refer to trusted individuals with access to organizational assets. Employees, partners, individuals with temporary access can easily misuse valuable data, conduct acts of sabotage, or unintentionally cause damage through digital means.

MAN IN THE MIDDLE

Man - In - The - Middle attacks intercept and alter the communication. Attackers exploit weaknesses to alter the data on the fly and manipulate them.