

DATE: 25 AUGUST 2026

1 Mongolia (Source: PIB)

- **Location:** It is a landlocked country in East Asia.
- **Capital:** Ulaanbaatar
- **Border Countries:** China and Russia
- **Geography**
- **Grasslands:** Mongolian-Manchurian grassland
- **Desert:** Gobi Desert
- **Population:** It is the world's most sparsely populated sovereign state.
- **Culture:** Tibetan Buddhism



2 Types of Cyber Attacks (Source: The Indian Express)



TYPES OF CYBER ATTACKS



Cyber attacks are malicious attempts to access, steal, alter, disable or destroy systems, data or networks.

1  MALWARE Malicious software designed to damage, disrupt or gain unauthorized access to a system.	 PHISHING Fraudulent attempts to trick users into revealing sensitive information like passwords or credit card details.
3  RANSOMWARE Malware that locks or encrypts your data and demands payment (ransom) to restore access.	4  DENIAL OF SERVICE (DoS / DDoS) Overwhelms a system, server or network with excessive traffic, making it unavailable to legitimate users.
5  MAN-IN-THE-MIDDLE (MITM) Attacker secretly intercepts and possibly alters the communication between two parties.	6  SQL INJECTION Exploits vulnerabilities in web applications to interfere with the database and access or manipulate data.
7  CROSS-SITE SCRIPTING (XSS) Injects malicious scripts into trusted websites, which are executed in the browser of other users.	8  ZERO-DAY EXPLOIT Attacks that target previously unknown vulnerabilities in software or systems before a fix is available.
9  PASSWORD ATTACKS Uses brute force, dictionary attacks or credential stuffing to guess or steal passwords.	10  INSIDER THREATS Malicious or negligent actions by trusted insiders (employees, partners) that compromise data or systems.
11  BOTNET ATTACKS Networks of infected devices (Bots) controlled by attackers to perform malicious activities without users' knowledge.	12  ADVANCED PERSISTENT THREAT (APT) Long-term, targeted attacks by skilled adversaries to steal data or spy on organizations silently.

PROTECT YOURSELF



Keep software and systems updated



Use strong, unique passwords



Be cautious of suspicious emails and links



Enable multi-factor authentication (MFA)



Regular security awareness and training