CAPTCHA

Source: TH

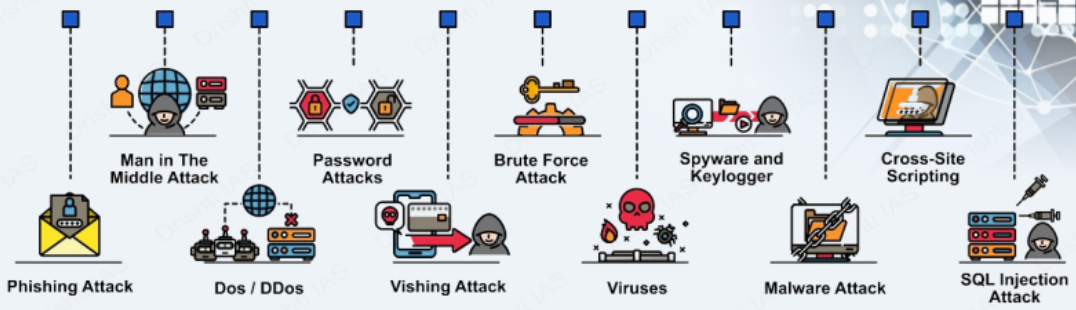
CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a **challenge-response test** used to **distinguish bots from human users**, enhancing online security and protecting user data.

- **Bots** are automated software programs that **perform repetitive online tasks.**
- **CAPTCHA:**
  - **Origin:** Developed in the early 2000s by **Luis von Ahn** to block bots, CAPTCHA began with **distorted text (2003),** evolved into **reCAPTCHA (2009)** using scanned book words, and later to **Invisible reCAPTCHA (2014) by Google** using behavioural analysis. Modern versions use **image recognition, checkboxes, and interaction tracking.**
  - **Advantages:** It **blocks bots preventing fake accounts, spam,** and data theft, ensuring only human users access digital platforms.
  - **Applications:** CAPTCHA is used in **logins, registrations, transactions, comments, account recovery,** and **surveys to block bots** and verify users. **reCAPTCHA** also aids in **book digitisation.**
  - **Disadvantages:** It can **hinder accessibility for disabled users,** can be **tedious for mobile users** and be bypassed by advanced bots, impacting user experience.
- **Other Cybersecurity Measures:** Other measures include **Two-Factor Authentication (2FA)**, adding a second verification layer via device codes, **biometric verification** using fingerprints or facial recognition, **honeypots** to trap bots; and **behavioral biometrics** that track typing or swipe patterns to distinguish humans from bots.

CYBER SECURITY

Cybersecurity refers to any technology, measure, or practice for preventing cyberattacks or mitigating their impact.

CYBER SECURITY ATTACKS



'Crime in India' Report 2022 (NCRB) highlighted 24.4% surge in cybercrimes in India since 2021.

Common Cybersecurity Myths

- Strong passwords alone are adequate protection
- Major cybersecurity risks are well-known
- All cyberattack vectors are contained
- Cybercriminals don't attack small businesses

Cyber Warfare

- Digital attacks to disrupt vital computer systems, to inflict damage, death, and destruction.

CYBER THREAT ACTORS

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Types of Cybersecurity

- Critical infrastructure security (Robust access controls)
- Network security (Deploying firewalls)
- Application security (Code reviews)
- Cloud Security (Tokenization)
- Information security (Data masking)

Recent Major Cyber Attacks

- WannaCry Ransomware Attack (2017)
- Cambridge Analytica Data Breach (2018)
- Financial data of 9M+ cardholders, including SBI, leaked (2022)

Regulations & Initiatives

- **International:**
  - UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace
  - NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - Budapest Convention on Cybercrime, 2001 **(India not a signatory)**
- **India:**
  - IT Act, 2000 (Sections 43, 66, 66B, 66C, 66D)
  - National Cyber Security Policy, 2013
  - National Cyber Security Strategy 2020
  - Cyber Surakshit Bharat Initiative
  - Indian Cyber Crime Coordination Centre (I4C)
  - Computer Emergency Response Team-India (CERT-In)

Steps Needed for Cyber Security

- Network Security
- Malware Protection
- Incident Management
- User Education and Awareness
- Secure Configuration
- Managing User Privileges
- Information Risk Management Regime

Drishti IAS

Read More: [Emerging Cyber Threats and Their Implications]