Mains Practice Question

Q. Social Engineering attacks are not only becoming more common against Businesses and Small and Medium Enterprises, but they are also increasingly more sophisticated. Analyse how Social Engineering attacks pose challenge to internal security in India? (250 Words)

22 Apr, 2022 GS Paper 3 Internal Security

Approach

- Explain what are Social Engineering attacks
- Enumerate the types of Social Engineering attacks
- Elucidate how it poses a threat to internal security
- Conclude with suggestions for making India threat proof from these attacks

Introduction

Social Engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data.

Commonly, social engineering involves e-mail or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file.

Perhaps the most famous social engineering attack comes from the mythological Trojan War in which the Greeks were able to get in to the city of Troy and win the war by hiding in a giant wooden horse that was presented to the Trojan army as a gift of peace.

Body

Types of Social Engineering attacks are as follows

- **Baiting:** As its name implies, baiting attacks use a false promise to pique a victim’s greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.
- **Scareware:** Scareware involves victims being bombarded with false alarms and fictitious threats.
- **Pretexting:** Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.
- **Phishing:** As one of the most popular social engineering attack types, phishing scams are e-mail and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims.
- **Spear phishing:** Spear phishing is like phishing but tailored for a specific individual or organization.
- **Vishing:** Vishing is also known as voice phishing, and it's the use of social engineering over the phone to gather personal and financial information from the target.
- **Honey trap:** An attack in which the social engineer pretends to be an attractive person to interact with a person online, fake an online relationship and gather sensitive information through that relationship.

- **Rogue:** Rogue security software is a type of malware that tricks targets into paying for the fake removal of malware.

Social Engineering and internal security-

- According to 'Internet Security Threat Report', released by Symantec, India is the third most vulnerable country in terms of risk of cyber threats. Social Engineering attacks can target persons involved in intelligence, defence or any other security services, leading to compromise of internal security architecture.
- Attackers posing as trusted individuals can persuade to divulge confidential information, possessed by a government employee.
- In the world of intelligence, information is the principal currency and can be used by inimical elements for undermining India's National Security. For example, in June 2019, it was discovered that a Pakistani spy going by the Facebook name "Sejal Kapoor" had hacked into the computer systems of more than 98 personnel of various defence forces. Two viruses, Whisper and GravityRAT, were used with more than 25 Internet addresses to mask her actual identity. Compared to traditional methods of honey trapping, this operation was swift, clean, and without any physical risk to the enemy
- Malware and phishing attacks can lead to leakage of data and "distributed denial of service" in critical infrastructure sectors, which could impede functioning of health, finance, power grids and other services, thus, deeply impacting the internal security.
- In this digital age, misinformation could be easily spread by the use of social engineering attacks, which can have wider implications on the economy and social harmony.
- There are multiple exit and entry points in cyberspace and attack technology is outpacing defence technology day by day. Under such circumstances creating security infrastructure which is impermeable to social engineering attacks is the most challenging task for the government.

In India, it is imperative that cyber networks, software and cyber-physical systems, and other platforms should be cyber-secure. This requires a judicious mix of people, policies and technology, as well as robust public-private partnership.

Public sensitization, awareness campaigns and preventive response from institutions like the National Cyber Security Coordinator (NCSC), National Technical Research Organisation (NTRO), and Computer Emergency Response Team- India (CERT-In) can save India from such threats.