1. Google has warned 500 Indians on Phishing

Prelims Level: Science & Technology

Mains Level: GS-III Awareness in the fields of IT, Space, Computers, Robotics, Nano Technology, Bio-Technology and issues relating to Intellectual Property Rights.

Why in News?

- Google has recently announced that over 12, 000 people around the world have become victims of phishing.

About:

- Google sent out over 12,000 warning to users globally, including about 500 in India, during the three month period from July to September this year, alerting them on "government-backed" phishing attempts against them.
- Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
- Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has.
- The website, however, is bogus and set up only to steal the information the user enters on the page.
- Phishing emails are blindly sent to thousands, if not millions of recipients.
- By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage.

Types of Cyber Attacks:

- **Malware,** short for malicious software refers to any kind of software that is designed to cause damage to a single computer, server, or computer network. Ransomware, Spy ware, Worms, viruses, and Trojans are all varieties of malware.
- **Phishing**: It is the method of trying to gather personal information using deceptive e-mails and websites.
- **Denial of Service attacks:** A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks

accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

- **Man-in-the-middle (MitM)** attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.
- **SQL Injection**: SQL (pronounced "sequel") stands for Structured Query Language, a programming language used to communicate with databases.
- Many of the servers that store critical data for websites and services use SQL to manage the data in their databases.
- A SQL injection attack specifically targets such kind of servers, using malicious code to get the server to divulge information it normally wouldn't.
- **Cross-Site Scripting (XSS):** Similar to an SQL injection attack, this attack also involves injecting malicious code into a website, but in this case the website itself is not being attacked.
- Instead the malicious code the attacker has injected, only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website.
- Social engineering is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.

Why Cyber Security Needed?

- Photos, videos and other personal information shared by an individual on social networking sites can be inappropriately used by others, leading to serious and even life-threatening incidents.
- Companies have a lot of data and information on their systems. A cyber-attack may lead to loss of competitive information (such as patents or original work), loss of employees/customers private data resulting into complete loss of public trust on the integrity of the organization.
- A local, state or central government maintains huge amount of confidential data related to country (geographical, military strategic assets etc.) and citizens. Unauthorized access to the data can lead to serious threats on a country.

International Mechanisms regarding Cyber Crime:

- **The International Telecommunication Union (ITU)** is a specialized agency within the United Nations which plays a leading role in the standardization and development of telecommunications and cyber security issues.

- **Budapest Convention on Cybercrime** is an international treaty that seeks to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It came into force on 1 July 2004. **India is not a signatory to this convention**.
- **Internet Governance Forum (IGF)** brings together all stakeholders i.e. government, private sector and civil society on the Internet governance debate. It was first convened in October–November 2006.
- **Internet Corporation for Assigned Names and Numbers (ICANN)** is a non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. It has its headquarters in Los Angeles, U.S.A.

Government initiatives against Cyber Crime:

- **Cyber Surakshit Bharat Initiative:** It was launched in 2018 with an aim to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
- **National Cyber security Coordination Centre (NCCC):** In 2017, the NCCC was developed. Its mandate is to scan internet traffic and communication metadata (which are little snippets of information hidden inside each communication) coming into the country to detect real-time cyber threats.
- **Cyber Swachhta Kendra:** In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.
- Training of 1.14 Lakh persons through 52 institutions under the Information Security Education and Awareness Project (ISEA) – a project to raise awareness and to provide research, education and training in the field of Information Security. International cooperation: Looking forward to becoming a secure cyber ecosystem, India has joined hands with several developed countries like the United States, Singapore, Japan, etc. These agreements will help India to challenge even more sophisticated cyber threats.