2. YouTube alerts users on phishing attempts through emails

Prelims Syllabus: Information Technology

Mains Syllabus: 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?

- Video sharing platform YouTube has alerted users that hackers were sending them phishing emails with suspicious links that appear to come from an official YouTube email address.

About the News:

- YouTube retweeted screenshots of the phishing emails and warned users that they were coming from the address 'no-reply@youtube.com.'
- As the address used the YouTube domain name and the video in the screenshot was linked to an account named 'YouTube Team,' the chance of user confusion was high.
- The email told users that YouTube's policies were changing and shared a video that urged recipients to read a longer description by clicking on the link.

Recent Steps Taken in India 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 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.
- **Indian Cyber Crime Coordination Centre (I4C):** I4C was recently inaugurated by the government.
- **National Cyber Crime Reporting Portal** has also been launched pan India.
- **Computer Emergency Response Team - India (CERT-IN):** It is the nodal agency which deals with cybersecurity threats like hacking and phishing.
- **Legislations in India:**
  - ✓ Information Technology Act, 2000.
  - ✓ Personal Data Protection Bill, 2019.

International Mechanisms:

- **International Telecommunication Union (ITU):** It 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:** It 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 1st July 2004. India is not a signatory to this convention.

Types of Cyber Attacks:

Malware:

- It is short for malicious software and 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 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 kinds 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:

- It 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.