Cyber Threat to Mobile Banking

For Prelims: Digital Payments, cybersecurity threat, Computer viruses, Data Breaches, Denial of Service (DoS) attacks, Trojans, Malware.

For Mains: Cyber-attacks & their impacts.

Why in News?

According to a recent study, more people are inclining toward **digital payments and there is a rise in the number of people's interactions with their bank or bank accounts** happen through their smartphones.

- Further, this acceleration brings along with it a vulnerability: an increased threat of **cyberattacks** on mobile devices.

What are Cyber Threats?

- **About:**
  - A cyber or **cybersecurity threat** is a **malicious act that seeks to damage data, steal data, or disrupt digital life in general. It includes computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.**
- **Different Types:**
  - **Malware: 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 a 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.
  - **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.

What are the Issues of Cyber Threats on Mobile Banking?

- **Increasing Cyber Attacks:**

- A study by cyber security firm Kaspersky warns of an **increase in cyberattacks on Android and iOS devices in the Asia Pacific (APAC)** as more people switch to mobile banking in the region.
- **Use of Trojans &** Malware:
    - As per Kaspersky, mobile banking **Trojans are dangerous malware that can steal money from mobile users' bank accounts by disguising the malicious application as a legitimate app** to lure unsuspecting people into installing the malware.
    - For e.g, mobile banking trojan, called **Anubis, has been targeting Android users since 2017.**
        - Further, its **worldwide campaigns have hit users in Russia, Turkey, India, China, Colombia, France, Germany, the U.S., Denmark, and Vietnam.**
- **Methodology:**
    - The perpetrators **infect the device through legitimate-looking and high-ranking malicious apps on Google Play, smishing (phishing messages sent through SMS), and BianLian malware,** another mobile banking Trojan,
        - Roaming Mantis is another prolific malware targeting mobile banking users.
            - The group attacks Android devices and spreads malicious code by hijacking domain name systems (DNS) through smishing exploits.

- **Interoperability issue:**
    - As various payment platforms like **Google Pay, PaytM, PhonePe, Square, PayPal, and Alipay have benefited from changes in consumer behaviour by adopting mobile banking.**
        - As a result, they have also permanently changed the payments game to their advantage.
    - **Closed Loop Payment System:**
        - These platforms are operating in a **closed-loop payment world where a Google Pay user can send money to another bank account via only the search giant's payment platform.**
            - It is similar to how Visa and Mastercard operate as they let payment transactions happen only within their own networks, not between each other.
    - **Change in Business Model:**
        - It's driven partly by **regulators that prefer open, standardized platforms that lower barriers to entry.**
        - Some countries are already making payment platform providers change their business models.
            - China, for instance, has ordered its **internet companies to offer their rival firms link and payment services on their platforms.**
            - In India, a **new law demands all licensed mobile payment platforms be capable of providing interoperability between wallets.**
        - The push from regulators to make payment platforms interoperable comes at a time when the demand for technical experts is a serious concern in the banking industry.
- **Shortage of Security Experts:**
    - The **shortage of technology, engineering, data and security experts needed by banks to realise their digital aspirations tends to hide a much wider problem**: banks' appeal as first-choice employers of all kinds of talent have faded.
- **Lack of Adequate Cybersecurity Policy:**
    - The lack of adequate cybersecurity and the dearth of talent in banking could potentially lead to a further rise in cyberattacks on user devices.
        - And until this mismatch is fixed, it helps to be careful and extremely cautious when using a mobile device to make payments.

Way Forward

- **Usual practice of digital hygiene** like keeping the phone up-to-date and rebooting regularly can be done.

- Further, consumers can ensure that they use **their phones for banking only** when the device is connected to a secure VPN (**VPN** stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks) and iOS 16 users can turn on Lockdown Mode as it limits the device's functionality and protects it from any potential malware.

UPSC Civil Services Examination Previous Year Question (PYQ)

Prelims

Q. The terms 'WannaCry, Petya and EternalBlue' sometimes mentioned in the news recently are related to (2018)

(a) Exoplanets
(b) Cryptocurrency
(c) Cyber-attacks
(d) Mini satellites

Ans: (c)

Exp:

- Ransomware is a form of malicious software (or malware). Once it takes over the computer, it threatens user to harm, usually by denying access to data. The attacker demands a ransom from the victim, promising to restore access to the data upon payment. WannaCry, Petya and EternalBlue are few of the ransom ware, which created havoc by demanding the victim ransom payment in bit coin (crypto currency).
- Cryptocurrency is a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. **Therefore, option (c) is the correct answer.**

Mains

Q. Discuss the potential threats of Cyber-attack and the security framework to prevent it. **(2017)**

Source: TH