Govt's Warning Against Phishing Attacks: RSTV- Big Picture

Anchor - Frank Rausan Pereira

Guests - Arvind Gupta, Head & Co-Founder, Digital India Foundation; Subimal Bhattacharjee, Cyber Security Expert; Karnika Seth, Cyber Law Expert.

What's in the News?

- India's official cybersecurity agency Cert-IN warned of a large-scale cyber-attack targeting 2 million individual email IDs belonging to users in India, specifically the residents from Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad .
- The warning is based on the findings of Cyfirma, a Singapore based cyber intelligence firm and has been attributed to the notorious North Korea backed cybercrime group- Lazarus Group.
- The attackers will send fake emails, social media posts or text messages related to COVID-19 to the targets, in order to steal their credentials, financial information or compromise their computers.
- These phishing campaigns will impersonate Government agencies, local departments that are responsible for disbursement of the government financial aid.
- These malicious emails could be sent through spoofed addresses – e.g.- ncov@gov.in. They could include links or files that can deliver malicious code.
- These malicious emails will have the subject line --
  - For example, --Signup for free COVID-19 testing.
- Detailed information could be asked from the targets such as - PAN no./communication address/health conditions.

Background

- Since the outbreak of COVID-19 pandemic in China, reports of phishing emails sent in the name of WHO, CDC and other government agencies for offering information, symptoms checking, free testing and seeking donations have increased.
- As per Cyfirma's report, Lazarus group plans to target nearly 5 million individuals and businesses in 6 countries including those in India between June 20 and June 21, 2020.

What are Phishing Campaigns?

- Coined in the mid 90s, the term phishing refers to fraudulent attempts to steal money and sensitive information such as usernames, passwords or credit card details of people or organisations by impersonating oneself as a trustworthy entity through an electronic communication means.
- Phishing attacks are cyber security threats of malicious intent, performed through social engineering techniques.
- Common motives behind phishing:
  - Financial Access
  - Identity theft
  - Installing malware - virus, worm, trojan horse, spyware, ransomware
  - Spreading misinformation and disinformation
  - Psychological Warfare - Through **Vishing** (Using Telephone) and **Smishing (**SMS**)**
  - Sexual exploitation of minors
- Types/techniques of phishing:
  - Spear Phishing
  - Whaling

  - Catfishing/Catphishing
  - Clone Phishing
  - Voice Phishing
  - Link Manipulation
  - Website Forgery

How to Identify a Phishing Attack?

- If the email or text message is coming from an unknown sender or a sender whose name is known but with whom one does not communicate normally.
- When an email has charged or alarmist language to create a sense of urgency, asking one to click and "act now" before one's account is terminated.
- The message contains unexpected or unusual attachments. These attachments could contain malware or ransomware.
- Misspellings in otherwise familiar looking websites or wrong embedded links.
- If one suspects an email is not legitimate, one can take a name or some text from the message and put it into a search engine to see if any known phishing attacks exist using the same methods.
- One can mouseover any doubtful link to see if it's a legitimate link or not.
- Differentiating between genuine and fake information - Genuine emails never ask for personal information or bank details of the customer. Fake emails can promise unexpected money or rewards and ask for bank or credit card details. They may also enquire Aadhar number, Pan number, address or demand money.

Psychological Tricks - Use of Clickbait Strategy for Phishing - Psychological tricks are where attackers play with the minds of the user to trap them with attractive offers. Once trapped, the attackers steal either money or sensitive information.

- Lottery Fraud - Attacker congratulates the victim for winning a lottery amount via e-mail/call/SMS
- Credit/Debit Card Fraud - Attacker scares the victims by informing them that their credit/debit card has been blocked to get them panicky. The attacker then exploits this situation to divulge sensitive personal information by promising to re-activate the card.
- Employment Related Fraud - Fake emails regarding attractive salaries.

How to Prevent/Protect against Phishing Attacks?

There are 2 aspects towards preventing widespread phishing the world over, which has especially increased since the outbreak of the COVID-19 pandemic. Hackers are devising strategies to capitalise on the fear and panic among people during the current situation.

- **Cyber Awareness Among Consumers/Citizens-** Large scale awareness campaigns need to be conducted by banks, corporates and Government agencies to educate people on the varied strategies of cyber security.
  - A user friendly Two Factor Authentication technology.
  - Never allow browser to store your username/password, especially if you use a shared computer device
  - 'File shredder software' should be used to delete sensitive files on computers
  - Take cognizance of cyber stalking. File complaint against the cyber stalker with National Cyber Crime Reporting Portal/Police. Also save all communications with the stalker, as evidence.
  - Social Distancing- Be careful while accepting friend requests from strangers on social media.
  - Never give out personal information through emails
  - Do not use Wi-Fi hotspots as far as possible to avoid being a victim of 'Auto Geo-tagging'.
  - Not forwarding fake emails or text messages without confirming its authenticity.

- **Institutional Level** - All large scale organisations are following Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol for email authentication. They are also using techniques like:
    - **Domain Keys Identified Mail (DKIM)**- An email authentication technique which allows the receiver to check that an email was indeed sent and authorized by the owner of that domain by giving email a digital signature.
    - **Sender Policy Framework (SPF)**- An email-authentication technique which is used to prevent spammers from sending messages on behalf of your domain.

Challenges in Tackling Trans border Cyber Crimes

- Lack of internationally agreed standards or multilateral conventions for criminalizing harmful acts of breaching cyber security.
- Most nations lack adequate laws governing criminalization of computer crimes. Only a few attackers are punished, that too after lengthy investigations. A large number of convicts continue to remain scot free.
- Attackers exploit the transnational character of the information infrastructure by launching attack packets from countries with inadequate laws, and perpetuating them through countries with totally different laws and practices. The scope of mutual cooperation between such countries is low.
- Dual criminality- Extradition is not allowed unless an act constitutes a crime under the laws of both the countries - one which is requesting extradition and the other from which extradition is being requested.
- Bilateral treaties between countries define their standards on transnational cyber terrorism.

Laws/Frameworks to Deal with Cyber Crimes in India

According to Karnika Seth, Cyber law expert - “Challenge is not lack of laws but a lack of effective implementation of the laws”.

Important provisions for protection against phishing:

- **Information Technology Act (IT Act) 2000 -** The aim of the Act is to provide legal recognition to transactions carried out by means of electronic data interchange and other means of electronic communications, commonly known as electronic commerce. Sections of IT Act 2000, dealing with punishment for cyber crimes-
    - **Section 65** - Tampering with computer source documents.
    - **Section 66** - Computer related offences.
    - **Section 66A, 66B , 66 C, 66 E, 66F -** Sending offensive messages, Dishonestly receiving stolen resource, Identity theft, Violation of personal Privacy, Cyber terrorism.
    - **Section 67, 67A, 67B , 67 C -** Publishing or transmitting obscene material, Failure to preserve and retain information by intermediaries.
- **Information Technology Act (Amendment) 2008 -** It empowers the Indian government to intercept, monitor and decrypt computer systems, resources and communication devices.
- **National Cyber Security Policy 2013 -** Framework by Department of Electronics and Information Technology. Main objectives:
    - To create a secure cyber ecosystem in the country
    - To enable effective prevention, investigation and prosecution of cybercrime
    - Creating mechanisms for Security Threats, Early Warning, Vulnerability management and response to security threats.
    - Promotion of Research and Development in cyber security.
- **RBI Rules 2017 -** For limiting the customer liability in case of unauthorised electronic banking transactions, RBI issued new directions under “Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions”.

  - Customers will not suffer any loss if unauthorised electronic banking transactions are reported within three days and the amount involved will be credited in the accounts concerned within 10 days.
  - In case the third-party fraud is reported with a delay of four to seven working days, a customer will face liability of up to Rs 25,000.
  - If the fraud is reported after seven days, the maximum liability of a savings bank account customer will be Rs 10,000.
  - Any loss occurring after reporting of the unauthorised transaction will be borne by the bank.
  - The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered.

Remedial Initiatives for Cyber Attack Victims

- In case of credit card details theft/lost or stolen mobile phones:
  - Get the card blocked immediately by informing the respective bank.
  - Take a screenshot of the amount debited notification as a digital proof of phishing.
  - Register an FIR with the police in case of phones, personal documents being stolen or PAN/AADHAAR numbers being accidentally shared.
- Sections 43 & 46 of Information Technology Act 2000 deal with reimbursements granted to the victims in incidents of cyber frauds. The Secretary (Information & Technology) grants compensation to the victims.
- **Banking Ombudsman Scheme 2006 (As amended upto July 1, 2017) -** A quasi judicial authority created to enable resolution of complaints of customers of banks relating to certain services rendered by the banks. There are 22 regional offices of the Banking Ombudsman in India.

Where to Report a Cyber Fraud?

- For reporting cybercrime complaints online- National Cyber Crime Reporting Portal should be contacted- **https://cybercrime.gov.in**/. The portal contains 2 sections--
  - For reporting crimes related to Women and Children (where reports can be filed anonymously as well).
  - For reporting other types of cyber crimes.
- Fraud sms, e-mail, link or phone call asking sensitive personal information or bank details can be complained of at www.report phishing.in.
- Latest advisories by CERT-IN should be referred to.