SOUTH INDIAN Bank

Experience Next Generation Banking

STUDENTS' ECONOMIC FORUM

A monthly publication from South Indian Bank

To kindle interest in economic affairs…
To empower the student community…

www.southindianbank.com
Student's Corner

ho2099@sib.co.in

CYBER FRAUDS

TYPES OF THREATS AND ATTACKS

AUGUST 2020 | THEME 345

29th Year of Publication

SOUTH INDIAN Bank

Experience Next Generation Banking

SIB PAYMENT GATEWAY SERVICES

A one stop solution for accepting payments online in the most convenient, simple, fast and secure mode.

SIB PAYGATE

FEEBOOK

- **Net Banking** 45+ Banks
- **Wallets** 15+ Major wallets
- **Credit / Debit Cards** (Visa, MasterCard, American Express, Rupay)
- **BharatQR**
- **UPI**

Features

Website integration of your firm for Payment Gateway services | SMS Invoicing | E-mail Invoicing | Smart Analytics | Merchant Dashboard

For more details, contact your nearest South Indian Bank branch.

Toll Free (India): 1800-102-9408, 1800-425-1809 (BSNL), Email: customercare@sib.co.in, CIN: L65191KL1929PLC001017

www.southindianbank.com | /thesouthindianbank

SOUTH INDIAN Bank
Experience Next Generation Banking

Theme No: 345: **CYBER FRAUDS: TYPES OF THREATS & ATTACKS**

"When learning is purposeful, creativity blossoms. When creativity blossoms, thinking emanates. When thinking emanates, knowledge is fully lit. When knowledge is lit, economy flourishes."
- Dr. A.P.J. Abdul Kalam

The "SIB Students' Economic forum" is designed to kindle interest in the minds of younger generation. We highlight one theme in every monthly publication. Topic of discussion for this month is **"Cyber Frauds: Types of Threats & Attacks".**

We are living in a digital era. Whether it be booking a hotel room, ordering food or even booking a cab we are constantly using the internet and inherently generating data. This data is generally stored on the cloud which is basically a huge data server or data centre that you can access online. Also, we use an array of devices to access this data. Now for a hacker, it is a golden age with many access points, public IP addresses, constant traffic and tons of data to exploit. Financial cyber-crime has become a real-and-present danger with the increasing adoption of online banking, mobile banking, fintech apps, and credit and debit cards in the country. From the simple to the sophisticated, cyber-criminals employ a range of tools to commit financial fraud. These conmen are an ingenious lot, always on the look-out for vulnerabilities and ways to exploit them. Things have got worse with the pandemic. In a world disrupted by Covid-19, financial fraudsters are on the prowl, preying on the emotionally and financially vulnerable. The fraudsters are employing many methods - some new and some time-tested. They are also quick, using day-to-day developments. Let's go through some of the most common types of cyber-attacks.

Cyber Threats

The cyber threats can be generally divided into 3 types.

1. **Cybercrime** includes individuals or groups targeting systems for financial gain or to cause disruption.
2. **Cyber-attack** often involves politically motivated information gathering.
3. **Cyber terrorism** is intended to undermine electronic systems to cause panic or fear.

Types of Cyber Threats

1. **Phishing, Vishing, Smishing**
   In **phishing,** conmen 'fish' or 'phish' (seek to extract) for your confidential information such as passwords, personal identification number (PIN), card verification value (CVV) and OTP. Phishing happens over email, and is one of the most widely used tricks. **Vishing** is short for 'voice phishing' and SMShing (also called **smishing**) is phishing through SMS. In vishing, the conman tries to extract your confidential information over the phone, while in smishing, he attempts to trick you via phone messages.
2. **Denial of Service (DoS) and Distributed Denial of Service (DDoS**
   Denial-of-Service attack (DoS attack) is a cyber-**attack** where the perpetrators

attempt to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial-of-service (DoS) attacks typically flood the servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them. It typically uses one computer and one internet connection to flood a targeted system. On the other hand, Distributed denial of service (DDoS) attacks are launched from multiple connected devices that are distributed across the Internet.

3. **Malware** - Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

   There are different types of malware, including:

- **Virus:** A self-replicating program that attaches itself to a clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:** Network of malware infected computers which cybercriminals use to perform tasks online without the user's permission.
- **Ransomware:** Another form of malicious software, is also a type of attack on availability. Its goal is to lock and encrypt your computer or device data - essentially holding your files hostage - and then demand a ransom to restore access. A victim typically must pay the ransom within a set amount of time or risk losing access to the information forever. Common types of ransomware include crypto malware, lockers and scareware. "Wannacry" or "WannaCrypt" is a popular example of Ransomware attack. WannaCry encrypts the computer's hard disk drive and then spreads laterally between computers on the same LAN. The ransomware also spreads through malicious attachments to emails.

4. **Identity Theft** - It is the deliberate use of someone else's identity, usually as a method to gain financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personal identity information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

   Common ways of Identity Thefts are:

   Shoulder surfing occurs when someone watches over your shoulder to nab valuable information such as your password, Debit/Credit Card PIN or number, as you key it into an electronic device. When the snoop uses your information for financial gain, the activity becomes identity theft.

   Dumpster diving involves searching through trash or garbage looking for

something useful. Dumpster-diving thieves go through your trash because they know the documents you discard as garbage contain personal identity information that can be spun into gold when used in a variety of illegal manner.

5. **SQL injection** - An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a database via a malicious SQL statement. This gives them access to the sensitive information contained in the database.
6. **Man-in-the-middle attack (MitM)** - Man-in-the-middle 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.

   Two common points of entry for MitM attacks:

   a). On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.

   b). Once malware has breached a device; an attacker can install software to process all of the victim's information.
7. **Pharming** - Cybercriminals install malicious code on your computer or server. The code automatically directs you to bogus websites without your knowledge or consent. The goal is to get you to provide personal information like payment card data or passwords, on the false websites. This cybercrime is also known as 'phishing without a lure'.
8. **Advanced Persistent Threat (APT)** - It is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APTs are advanced attackers who have access to significant financial and technical resources. These attackers are typically sponsored by government/military agencies or large organized crime rings. They conduct research to identify previously unknown vulnerabilities and exploit those vulnerabilities to gain access to systems in an undetected manner.
9. **Brute force** - (also known as brute force cracking) is a trial and error method used to decode sensitive data. The most common applications for brute force attacks are cracking passwords and cracking encryption keys, through exhaustive effort (using brute force) rather than employing intellectual strategies.
10. **Click jacking** - (also known as User Interface redress attack) is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly harmless objects, including web pages.
11. **Web jacking** - is a phishing technique which is used in social engineering engagements. Attackers use this method to create a fake website and when the victim opens the link, a page appears with the message that the website has moved and they need to click another link. Here, the hacker takes control of a web site fraudulently.
12. **Juice jacking** or USB charging scam - refers to data theft through USB charging points. Public facilities like airports, railway stations, malls and restaurants are providing charging points where USB cables can directly be connected for charging and there is threat of data theft or device infection through these unchecked and uncontrolled points.
13. **Drive by downloads** – It refers to the unintentional download of malicious code to a user system that exposes users to cyber-attacks. It usually takes advantage of a

browser, app or operating system that is out of date and has a security flaw.

14. **Cross Site Scripting** - A type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. These attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

In News

» India has seen a 37 per cent increase in cyberattacks in the first quarter (Q1) of 2020, as compared to the fourth quarter (Q4) of last year, a new report revealed.
The Kaspersky Security Network (KSN) report showed that its products detected and blocked 52,820,874 local cyber threats in India between January to March this year.
The data also shows that India now ranks 27th globally in the number of web-threats detected by the company in Q1 2020 as compared to when it ranked the 32nd position globally in Q4 2019.

» Cyber security attacks and breaches in the country may have jumped by as much as 500% since the lockdown was first announced in March, according to security experts. Internet service providers receive cyberattack alerts from corporate clients almost every alternate day compared with an average of once a week before lockdown was announced.

» In the beginning of July, banks such as SBI and ICICI started warning their account holders of an imminent cyber-attack. This was on the basis of an advisory from the Indian Computer Emergency Response Team (CERT-In), that cyber-criminals are planning to send malicious emails claiming to be from the government — promising free and mandatory Covid-19 testing.

» There has been a sharp increase in the number of ransomware attacks on Indian organisations, and with that the ransomware kitty has also witnessed a spike. According to a recent survey, Indian organisations have incurred costs of around ₹8.02 crore to rectify the impact of each ransomware attack, hinting at the seriousness of the cyber-attack. However, only 8 per cent of victims were able to stop the attack before their data could be encrypted, compared with a global average of 24 per cent. While one-third of respondents said they could recover the (stolen) data from back-ups without having to pay a cent to the hackers, 66 per cent of the organisations said they paid ransom to get the data released.

» Another report says that India ranks third place in the most significant cyber-attacks, falling prey to 23 significant cyber-attacks. In their latest cyber-attack, in June 2020, the country experienced a high-profile attack where malware was deployed against nine human rights activists to log their keystrokes, record their audio, and steal their personal credentials.

» Hackers based in China attempted over 40,000 cyber-attacks on India's Information Technology infrastructure and banking sector during last week of June. The spurt in online attacks from across the border was noticed after tensions rose between the two countries in eastern Ladakh. 'Maharashtra Cyber', the state police's cyber wing, collated information about these attempts and most of them were found to have originated in Chengdu area in China. The attacks aimed at causing issues such as denial of service, hijacking of Internet Protocol and phishing.

Reference: Cisco, Kaspersky, Norton, Business line, Economic times, Edureka

SOUTH INDIAN Bank

Experience Next Generation Banking

Discover a world of convenience with SIB Debit Cards.

RuPay Platinum EMV International

MasterCard Business Platinum EMV International

VISA Platinum EMV NFC International

MasterCard World EMV International

Toll Free (India): 1800-102-9408, 1800-425-1809 (BSNL), Email: customercare@sib.co.in, CIN: L65191KL1929PLC001017

www.southindianbank.com | /thesouthindianbank

SIB INSTA

No forms to fill. No queue.
Presenting SIB Insta - a savings account for those living life on the fast lane.

- **Instant account opening**
- **No physical documentation**
- **No minimum balance commitment**
- **Get 200 reward points & a free personalised Debit Card on initial remittance of Rs.1000/-**
- **Option to select branch of your choice**

Prerequisites:
Aadhaar and PAN Card.

To know more,
scan the QR code

SOUTH INDIAN Bank
Experience Next Generation Banking

Toll Free (India): 1800-102-9408, 1800-425-1809 (BSNL), Email: customercare@sib.co.in, CIN: L65191KL1929PLC001017
www.southindianbank.com | /thesouthindianbank