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 SECURITY – THE NEW AGE SECURITY

OCTOBER 2022 | THEME 370

32nd Year of Publication

SIB introduces

Video KYC Account Opening.

Banking Simplified

Aadhaar + PAN Card + Video Call
to open your SIB Video KYC Account

T&C apply

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

www.southindianbank.com | /thesouthindianbank

"True Cybersecurity is preparing for what's next, not what was last"
Neil Rerup

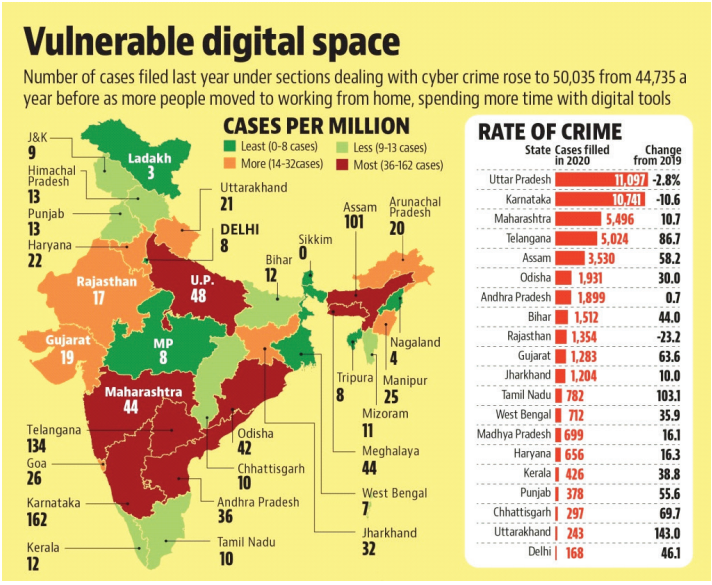
The "SIB Students' Economic forum" is designed to kindle interest in the minds of younger generation. We highlight one theme in every monthly publication. Topic of discussion for this month is "**Cyber Security – The New Age Security**"

The New Age Security

The Digital Era has opened doors to a digital landscape like never before. Today the Internet of Things has taken over and is going above and beyond to what man can expect out of technology.

Just when we feel that technology has reached its best, a new invention / innovation come into the market, some of which even have the power to make earlier systems obsolete. Video game consoles, watches, mobile phones, cameras, televisions, security systems, automobiles and many more have all been made so integrated with each other that data/information has become easier to transfer from one device to another.

Further, e-commerce has broadened the scope of applicability of such devices. As we rely more and more on such devices, there may be requirements for us to share crucial information about us as well as about others. This raises the question of safety and security of the data which is being shared in the digital ecosystem and hence Cyber Security becomes the need of the hour.



(Source : Hindustan Times)

Understanding Cyber Security

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorized exploitation of systems, networks, and technologies.

The Minister of State for Electronics and Information Technology, Mr. Rajeev Chandrasekhar, has informed that over 6.74 lakh cyber security incidents were reported in India till June 2022. More than 14 lakh cyber security incidents were observed in the year 2021.

248 data breaches were reported to RBI by private as well as state owned banks during the period between June 2018 and March 2022. The reasons behind cyberattacks might be many like for unauthorised extraction of business' financial details, customers' financial details, sensitive personal data, customer databases, warfare, making a social or political point (eg Hacktivism), spying on competitors for unfair advantage (espionage) and many more.

Common Types of Cyber Attacks

S No	Name of Cyber Attack	Nature of Attack
1.	Card Skimming	Card skimming is the theft of credit and debit card data and PIN numbers when the user is at an automated teller machine (ATM) or point of sale (POS). Card skimming allows thieves to steal money from accounts, make purchases and sell card information to third parties for the same purposes. Generally, the exploit involves modified payment card reader hardware that fits over an existing genuine payment device or ATM. The phony reader collects and passes on payment card information for retrieval by the thief. PIN numbers may be retrieved with a keypad overlay or a hidden camera.
2.	Denial-of-service (DoS)	DoS and Distributed denial-of-service (DDoS) attacks flood a system's resources, overwhelming them and preventing responses to service requests, which reduces the system's ability to perform. Often, this attack is a setup for another attack.
3.	Malware	Malware is malicious software that can render infected systems inoperable. Most malware variants destroy data by deleting or wiping files critical to the operating system's ability to run.
4.	Phishing	Phishing scams attempt to steal users' credentials or sensitive data like credit card numbers. In this case, scammers send users emails or text messages designed to look as though they're coming from a legitimate source, using fake hyperlinks.

5.	Ransomware	Ransomware is sophisticated malware that takes advantage of system weaknesses, using strong encryption to hold data or system functionality hostage. Cybercriminals use ransomware to demand payment in exchange for releasing the system. A recent development with ransomware is the add-on of extortion tactics.

Let's Cyber Secure Ourselves!!!!

Some simple ways to keep ourselves and our devices from cyber attacks are –

- **No Anti-virus means no safety** – Such softwares are useful to detect and hold attacks from external sources which comes from external devices or through the web.
- **Your Applications (Apps) needs to stay updated just like you** – Software makers regularly monitor their softwares for errors or scope for upgradation. This enhances the safety elements in these softwares as newer updates tend to correct the errors identified or help upgrade the software based on the latest requirements. This is also vital when it comes to Anti-virus and softwares used for protection against Cyber Threats.

- **Make your passwords not so obvious** – Using the first few letters of your name or other such simple combinations are easy to crack nowadays. Hackers go one step further even to find out your personal data so that they can crack your password combinations. Thus, use symbols such as *, ! , #, & etc along with a good combination of capital and small letters and numbers which preferably should not link to a name of your family member, pet or someone or something that you consider important.

  You may choose a password length as 12 or more and avoid using the same password in multiple locations. It is highly recommended that you change the password once in 30 days irrespective of prompt from the system. Never try to use any of the previously used password as current password.

- **Keep strangers away** – We recommend that you keep away from suspicious emails , messages and phone calls. Such communications have a tendency to slowly extract personal details along with money with or without our consent, once they find someone who responds to them.

- **Update yourself the way you update your device** – Knowledge is free and widely available. Stay alert to the various incidents that happen near you. The Reserve Bank of India also circulates advertisements for creating Public Awareness through Print and other media for your safety.

- **Learn to keep secrets** - Passwords are never meant to be shared. So are OTPs or PIN numbers. Follow it as a rule of Thumb as the chances of being a victim of an attack would be substantially lower.

Cyber Attacked? What Next?

- Identify the source of attack – Doing so would help to disconnect oneself from being attacked further. Also it would help us to report the incident.
- Stop yourself from being attacked further – Disconnect your device from the source of attack. In case if the attack is done using your debit or credit card, you may quickly block the card calling the designated toll free number of the service provider.
- Report to your Bank – In case the attack involves targeting or loss of finance, then one must report of such an incident to his/her bank. This helps the bank to assess the situation and take the necessary preventive measures.
- Report to the government - Cyber Crimes may be reported to the Government of India in its portal (https://cybercrime.gov.in/). The Cyber crime helpline is 1930. This portal also shares information on the various types of cyber crimes.

https://www.techtarget.com/searchsecurity/definition/cybersecurity

https://inc42.com/buzz/over-6-7-lakh-cybersecurity-incidents-reported-in-india-in-the-first-six-months-of-2022/

https://www.itgovernance.co.uk/what-is-cybersecurity

https://www.nibusinessinfo.co.uk/content/reasons-behind-cyber-attacks

https://www.ibm.com/in-en/topics/cyber-attack

https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/

https://www.hindustantimes.com/india-news/cyber-crimes-registered-11-8-increase-last-year-ncrb-101631731021285.html

SIB SUPERFAST GOLD LOAN

You don't have to sell your favourite gold jewellery, when you can pledge it. With South Indian Bank's Superfast Gold Loan, you get the money to meet your different needs, really fast. It is a gold loan tailor-made for the uncertain times we are living in. Go ahead, encash your dreams with SIB Superfast Gold Loan.

- Easy processing
- Tenure up to 12 months
- Attractive interest rate

Wear masks in public spaces. Follow social distancing.

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

INTERNATIONAL ONLINE MONEY TRANSFER THROUGH INTERNET BANKING

Foreign Outward Remittance through SIBerNet Internet Banking

Features

Transaction limit:

Resident SB
Daily limit - USD 10000
Financial year - USD 25000

NRE SB
Daily limit - USD 25000
Financial year - USD 100000

Rate for conversion:
TT selling rate available at that point of time

Available currencies:
USD, EUR, GBP, CAD, JPY, AED, CHF, AUD, SAR, SGD & other 100+ currencies

Timings window:
24x7 for US dollar remittances
10 AM to 3 PM (IST) for other currencies

T&C apply

Purpose of remittance:

Active NRE SB with valid VISA expiry dates — Repatriation from NRE account (S0014)

Auto mailer of SWIFT copy will be sent to the registered email ID of the remitter on completion of transaction.

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