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

OVERVIEW & ONLINE SAFE GUARDS

SEPTEMBER 2020 | THEME 346

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

Theme No: 346: **CYBER SECURITY: OVERVIEW & ONLINE SAFE GUARDS**

"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 Security: Overview & Online Safe Guards".**

The Internet sure isn't a safe place as you might think it is. There have been multiple cyber breaches in the past that had compromised the privacy & confidentiality of data. This not only applies to individuals but also to large organisations. Big companies like eBay, AOL, Evernote, Adobe have actually gone through major cyber breaches even though they have tight security measures to protect data that they store. In the financial sector too, various big banks faced data breaches. So, there must be a mechanism for protection from these sorts of cyber-attacks and that is Cyber Security. The use of cyber security helps to prevent cyber-attacks, data breaches, identity theft and can aid in risk management. So, when an organization has a strong system of cyber security and an effective incident response plan, it helps to prevent and mitigate these attacks.

Cyber Security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is a subset of information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security,** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security,** focuses on keeping software/applications free of threats. A compromised application could provide access to the data it's designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security,** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security,** includes the processes and decisions for handling and protecting data assets. The permission which users have to access a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Cloud security,** protects and monitors your data in the cloud, to help eliminate the risks associated with on-premises attacks.
- **Database and infrastructure security:** Everything in a network involves database, operating system and physical equipment. Protecting these devices is equally

important.

- **Data loss prevention,** detects potential data breaches / data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use, in motion and at rest.
- **Disaster recovery and business continuity,** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan which the organization falls back on while trying to operate without certain resources.
- **End-user education,** addresses the most unpredictable cyber-security factor or the weakest link in cyber security front: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

The CIA Triad/ Pillars of Cyber Security

There are three main pillars of cyber security that we deal with since inception of the computers. They are Confidentiality, Integrity and Availability also known as the CIA triad.

1. The Principle of confidentiality asserts that information and functions can be accessed only by authorized parties. For example, when we password protect our files, we are trying to prevent other users from accessing our data and peeping into our files so that our data remains confidential. The attacks on confidentiality can be designed to steal our personal identifying information and our bank account or credit card information.
2. Integrity, this is where the trustworthiness of the data comes into the picture. It refers to preventing data from being tampered with, modified, or altered in an unauthorised way to achieve malicious goals. The data which is sent must be received intact and unaltered.
3. The availability part ensures that this data is made available to all authorized users when and where they want it. The principle of availability asserts that, functions and data must be available in systems on demand according to agreed-upon parameters based on levels of service. For example, when we login to Gmail, we always assume that Gmail is going to be available for us. What if it is not available when you want it?

How does cyber security work?

It's all about securing a computer and there are various methodologies. There are various factors involved in securing various aspects of the same computer.

➤ **Regular updates**

All the operating systems or the applications that you use will receive regular updates. It could be for functionality but more for security so as to detect new vulnerabilities in applications or operating systems. The software vendors or the software developers over a period of time start sending out these updates also called patches to the end users. It is very important for the end-users to identify the security patches and install them on their devices as soon as possible, else they remain open to those vulnerabilities and unpatched system that can easily be hacked.

➤ **Installing firewall on the system or a server**

A firewall is essentially the software or hardware that allows or disallows some functionality. For example, a port to be opened or closed or a service to function or not to function on a computer. Thus, what we are trying to do here by disabling unwanted services is, we are limiting the threat landscape that we're creating for our computer. If a service doesn't exist on your computer, it cannot be hacked. So, the essence here is to identify the ports and services which we will be using and then create a policy on the firewall to ensure that only required ports and services are running.

- **Usage of an antivirus**
  To protect yourself from viruses, worms, trojans, essentially malwares. You cannot rely on the operating system alone to protect you. So there has to be an antivirus which will scan the connections you make, the websites that you visit, the files that get executed in the background and ensure that everything happens in the proper way.
- **Securing our passwords**
  Just having a password may not be sufficient. We have to ensure that the password meets some complexity standards so that the security or complexity of the password is high enough and cracking programs will fail.

General characteristics of a strong password

a) At least 8 characters – the more characters, the better.
b) A mixture of both uppercase and lowercase letters
c) A mixture of letters and numbers
d) Inclusion of at least one special character, e.g.!@#$%&*?

- **2 factor Authentication**
  Authentication is the process or action of verifying the identity of a user or process. There is always a username and an associated password with it. The username is to identify the account that person wishes to access and Password is for "Authentication' and 'Authorizing'. (E.g. Customer facing applications such as Internet Banking, Mobile Banking etc. where login password is for authentication and transaction password/MPIN is for authorising the transaction). Now here we may want to enhance authentication mechanism by using a two-way authentication. For example, with banks, when we type in the username and password, they send an OTP or a one-time password which is auto generated by a server to a registered device that the person owns.
- **Cryptography/ encryption**
  The best way to keep everything secure is to encrypt it. However what kind of encryptions are required, what should be encrypted, what should not be encrypted, how the encryption should function, and how this encryption enhances the business value, is what we need to ensure. You first need to identify the protocols you're going to consume, what data is going to be transmitted, how valuable the data is to your organization and then encryption is to be done to prevent attacks from hackers.
- **Securing DNS servers**
  DNS is a domain name server which is basically an index that maps our domain names to our IP addresses. Now on the Internet, computers do not know domain names they can only identify IP addresses and MAC addresses. So, when we type in 'www.google.com' on our browser, the computer doesn't know what 'google.com' is. What it does is, it sends the packet to the DNS server and in the DNS server, it

enquires where 'google.com' is located. It is given the corresponding IP address because of which the packet then goes to the relevant server. There are attacks where a DNS can be compromised and the pointer pointing to your particular website can be changed to point to a malicious server that a hacker is hosting. So, to prevent that from happening you need to secure your DNS servers.

Key safeguards against cyber attacks

- Never share confidential data such as OTP, CVV, PIN, UPI MPIN, passwords.
- Register for both SMS and e-mail alerts for financial transactions. Check these alerts.
- Do not click suspicious links or open suspicious attachments.
- Do not click links or open e-mail attachments sent by unknown persons.
- Do not enable macros by default.
- Transact on websites with URLs starting with https (as against http) and having a padded lock icon.
- Share personal information with others only on a need-to-know basis.
- Buy genuine software.
- Update electronic devices with the latest anti-hacking and anti-virus protection.
- Use strong passwords and change them regularly.
- Use virtual keyboard and virtual cards wherever available for online transactions.
- Check for hidden cameras or devices at ATM enclosures.
- Enter PIN discreetly in ATMs or at physical stores.
- Download mobile apps from genuine sources only.
- Do not tamper with the security settings of your mobile phone.
- Be wary of emails/messages with spelling mistakes or grammatical errors.
- Be wary of emails in which the sender's email address is not the same as their display name.
- Be wary of emails/messages that tell you to act urgently or reply immediately.
- Do not forward suspicious SMSes.
- If your mobile phone telecom service stops for unknown reasons, check with your telecom service provider immediately.
- Avoid using public charging stations such as ones at airports. Carry your charging adapter or power bank.
- Avoid public computers for financial transactions.
- Avoid using unsecured Wi-Fi.
- Know what to do if you become a victim.

Over the last decade, cyber security has rapidly become a worriesome problem. Rightfully so, given how a cyber-attack can compromise an organization's key functions and processes within a matter of seconds, exposing sensitive data to opportunistic criminals. There is more than 500 per cent increase in cyber-attacks since the lockdown began, which illustrates how threat actors are rushing to take advantage of the current situation. A cyber security report predicts that the impact and severity of cyber-attacks can be huge and it will cost the global economy a shocking USD 6 trillion per year by 2021.

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