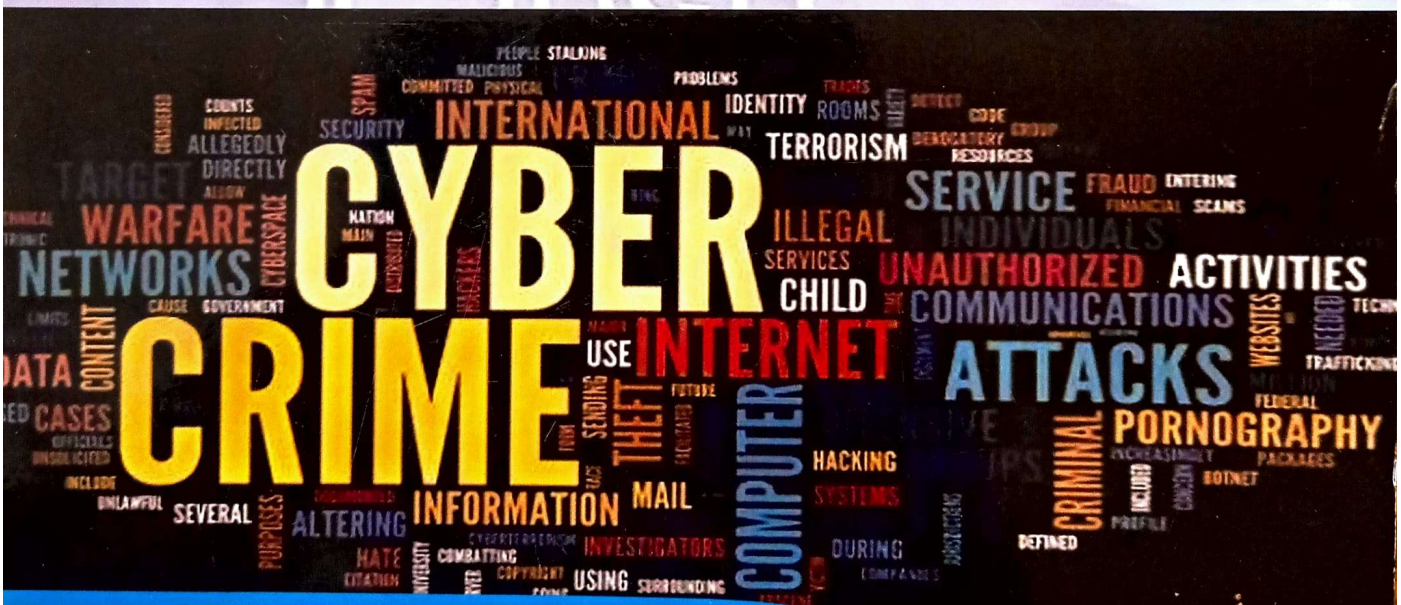
DIGITAL TRANSACTIONS AND CYBER CRIMES



Organised by : Department of Commerce

Smt. N.P. Savitramma Govt. Degree Colleg for Women,
Chittoor, Chittoor Dist., Andhra Pradesh

Dr. T. Vinila

SMT.N.P.SAVITHRAMMA GOVT DEGREE COLLEGE FOR WOMEN
CHITTOOR DIST. A. P

INVITES YOU TO
ICSSR SPONSORED
TWO- DAY NATIONAL SEMINAR

On

DIGITAL TRANSACTIONS AND CYBER CRIMES
(Under azadi ka amrit mahostav)

Organized
By
THE DEPARTMENT OF COMMERCE

12th &13th November,2022

Seminar Director

Dr.K.Manohar, Principal

Seminar Convenor

Dr.T.Vinila, Asst.Prof of Commerce

Seminar Convenor

A.M Narendra Kumar,Lecturer in Commerce

S.NO

CONTENTS

Pg. No

S.NO

CONTENTS

Pg. No

S.NO

CONTENTS

Pg. No

S.NO

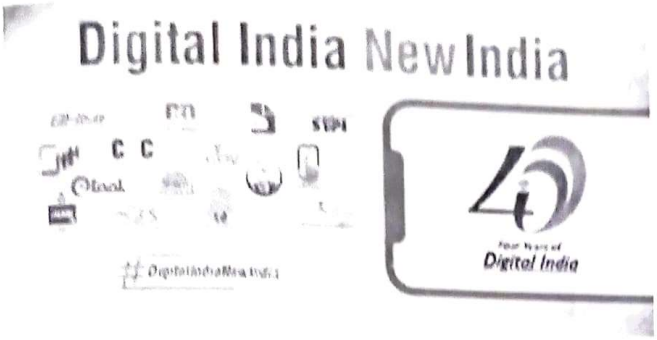
CONTENTS

Pg. No

17

DIGITAL INDIA – ISSUES AND CHALLENGES

P. RAMYA KRISHNA
Lecturer in Chemistry, Sir C R Reddy College for women, Eluru



ABSTRACT

The Information age has brought about a revolution in technological advancement. The industrial revolution propelled the world into a new era of greater mechanical advantage and shaped our current world. India was suffering with division and lack of political stability at that time and was not able to capitalize on its resources, then. So, when the world ushered into a new era of digitization, Digital India was launched to digitize the entire ecosystem and to make full use of our natural and human resources. Digital India aimed to capitalize on this opportunity by positioning ourselves in the best way possible. Although these programs have come a long way forward, they have faced major challenges. The successful launch and growth of E-governance platforms and other technological advancements are leaving many Indians behind and this divide is to be checked by increasing the digital literacy of the average Indian. Are the various programmes under this digital India scheme dealing with most of these problems and are they setting the stage for a bright and technically advanced future is to be seen.

About Digital India:

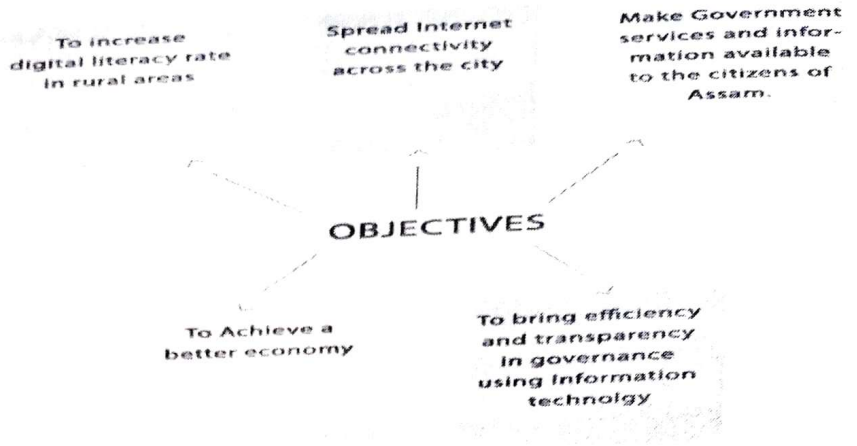
Digital India is a campaign launched by the Government of India in order to ensure the Government's services are made available to citizens electronically by improved online infrastructure and by increasing Internet connectivity or making the country digitally empowered in the field of technology.Launched on 1 July 2015, by Indian Prime MinisterNarendra Modi, it is both enabler and beneficiary of other key Government of India schemes, such as BharatNet, Make in India, Startup India, Standup India, industrial corridors, Bharatmala and Sagarmala. As of 31 December 2018, India had a population of 130 crore people (1.3 billion), 123 crore (1.23 billion) Aadhaar digital biometric identity cards, 121 crore (1.21 billion) mobile phones, 44.6 crore (446 million) smartphones, 56 crore (560 million) internet users up from 481 million people (35% of the country's total population) in December 2017, and 51 per cent growth in e-commerce.

Objectives of Digital India

The motto of the Digital India Mission is 'Power to Empower'. There are three core components to the Digital India initiative. They are digital infrastructure creation, digital delivery of services, and digital literacy.

The major objectives of this initiative are listed below:

1. To provide high-speed internet in all gram panchayats.
2. To provide easy access to Common Service Centre (CSC) in all the locality.
3. Digital India is an initiative that combines a large number of ideas and thoughts into a single, comprehensive vision so that each of them is seen as part of a larger goal.



Advantages of Digital India Mission

Digital India Mission is an initiative that encompasses plans to connect the rural areas of the country with high-speed internet networks. Public Internet Access Programme is one among the nine pillars of digital India. On the platform of digital adoption, India ranks amongst the top 2 countries globally and the digital economy of India is likely to cross $1 trillion by the year 2022.

Some of the advantages of Digital India are:

1. There is an increase in electronic transactions related to e-governance.
2. An optical fiber network of 2, 74,246 km has connected over 1.15 lakh Gram Panchayats under the Bharat Net programme.
3. A Common Service Center (CSC) is created under the National e-Governance Project of the Indian government which provides access for information and communication technology (ICT). Through computer and Internet access, the CSCs provide multimedia content related to e-governance, education, health, telemedicine, entertainment, and other government and private services.
4. Establishment of digital villages along with well-equipped facilities such as solar lighting, LED assembly unit, sanitary napkin production unit, and Wi-Fi choupal.
5. Internet data is used as a major tool for the delivery of the services and the urban internet penetration has reached 64%.

Nine pillars of Digital India are Broadband Highways, Universal Access to Mobile Connectivity, Public Internet Access Programme, e-Governance: Reforming Government through Technology, e-Kranti – Electronic Delivery of Services, Information for All, Electronics Manufacturing, IT for Jobs and Early Harvest Programmes. Each of these areas is a complex programme in itself and cuts across multiple Ministries and Departments.

Challenges of Digital India

The government of India has taken an initiative through the Digital India Mission to connect the rural areas of the country with high-speed internet networks. Apart from the various initiatives taken by Digital India, there are several challenges faced by it.

Some of the challenges and drawbacks of Digital Mission are mentioned below:

1. The daily internet speed, as well as the Wi-Fi hotspots, are slow as compared to other developed nations.

2. Most of the small and medium scale industry has to struggle a lot for adapting to the new modern technology.
3. Limited capability of entry-level smart phones for smooth internet access.
4. Lack of skilled manpower in the field of digital technology.
5. To look for about one million cyber security experts to check and monitor the growing menace of digital crime.
6. Lack of user education.

PROPOSED SOLUTIONS

With the increase in the digital infrastructure of the country, we have already seen the power that digitization yields in changing the face of a company, industry or country. Some of the solutions for better Digital growth are

1. Spreading Digital awareness
2. Empower people with knowledge rather than digitizing everything and hoping people will adapt.
3. Relentless marketing of government schemes in rural and urban areas alike will help the scheme gain momentum, market share and users.
4. Last but not the least, the internet speeds need to be checked and actions must be taken for violating trust and connection speeds.

CONCLUSION

The goal of Digital India is far away as most of the nine pillars of digital India mission are facing serious challenges in implementation. Persistent attention must be given to each and every pillar so that this programme does not be a failure project.

The following steps may be considered to fulfil the vision of Digital India

1. Digital literacy should provide knowledge to secure their online data.
2. Massive awareness is to be created particularly in rural areas.
3. Digital divide needs to be addressed.
4. This mission needs content and service partner ships with telecom companies and other firms to develop infrastructure.
5. The success of digital India project depends upon maximum connectivity with minimum cyber security risks. For this there should be a strong anti cyber crime team.
6. To improve skill in cyber security, cyber security courses should be introduced with academics.
7. There is need for effective participation of various departments and demanding commitment and efforts. Various policies in different areas should support this goal

REFERENCE:

1. Gupta andArora (2015) studied the impact of digital India project on India's rural sector.
2. The study found that many schemes have been launched in digital India to boost agriculture sector and Digital India : challenges and suggestions f or implementation volume – 8 issue October - 2018 Available online at www.lbp.world.entrepreneurship development in rural areas.
3. Digital India programme has also set the stage for empowerment of rural Indian women Singh (2015) began with the basic overview of what Digital India entails and led a discussion of conceptual structure of the program and examined the impact of "Digital India" initiative on the Technological sector of India. He concluded that this initiative has to be supplemented with amendments in labor laws of India to make it a successful campaign.

4. Midha(2016) concluded that digital India is a great plan to develop India for knowledge future but its improper implementation due to inaccessibility and inflexibility to requisite can lead to its failure.
5. Though digital India programme is facing number of challenges yet if properly implemented it can make the best future of every citizen. So we Indians should work together to shape the knowledge economy Pichai, Nadella, & Musk (2016) researched about Digital India and its preparedness to create jobs opportunities in the information sector. They concluded that creating new jobs should be continued with shifting more workers into high productivity jobs in order to provide long term push to the technological.
6. Gupta and Arora (2015) studied the impact of digital India project on India's rural sector. The study found that many schemes have been launched in digital India to boost agriculture sector.

DIGITAL PAYMENTS METHODS – PROBLEMS AND PROSPECTS

***P. NAGA LAKSHMI**
Department of Commerce, Sir C R Reddy College for Women, Eluru.

****K. ANAND RAO**
Department of Physics, Sir C R Reddy College, Eluru.

Abstract:

After demonetization initiatives, most of the people in India started electronic payments for conducting the transactions. Slowly India is moving towards cashless economy. A cashless economy is one in which all the transactions are done using cards or through digital means. The flow of physical currency is minimized in cashless economy. The benefits of cashless economy are many. Indian Government launched digital Indian Campaign to reduce dependency Indian economy on cash and prevent from money laundering. To making cashless India and increasing trends in using digital payment system various payment methods are emerging and developing. India is developing country, the minimum area is rural and shocking is computer literacy is only 6.5% then question arises that implementation of digital payment system. In this paper an attempt is made to focus on the problems of digital payment system in India and effects of the system on people and economic system of India. In this paper an attempt is also made to explain the future scope of the digital payment system.

Keywords:- *Demonetization, electronic payments, cashless economy & Digital India campaign, laundering.*

Introduction:-

Cashless society describes an economic state where financial transactions are not conducted with money in the form of physical bank notes (or) coins, but rather than digital currency, crypto currency is used. The digital payment system is now became the essential part of banking transaction. The digitalization is need of country because it is important to develop the financial sector as per the modern age requirement and to face the competitions with developing countries. The PM Narendra Modi started a mission digital India in 2017 for removing hidden money and black money from the country. The digital payment system is a part of the mission from this cashless transaction will made all over the India and progress black money ormoney laundering can be reduced. It is also important that development of techniques influences the traditional system and there also have to face some problems while newly adaption. In India ICICI Bank started the online banking services and digital bank is also a head in digitalization of transactions digital services provides to customer. SBI bank is a public sector Bank which is enriched of digitalization. In 2017 SBI launched green channel to promote digital payment system and save environment.

The traditional system is replacing by the digital system. The traditional payment systems are Cheques, withdrawals, drafts, money orders, letters of credits, travel chequesetc., why payment system also turning into electronic payment system using computer and internet there are several reasons of adoption. The most common reason is that the traditional system has some leakages and inefficiency and that's overcome by the digital payments system. But in India digital payment system is in emerging trend and not so popular and generalized.

Today India is using most common electronic payment systems include Debit Cards, Credit Cards, but the use of Electronic Fund Transfer, Internet Banking, Unified Payment System (UPI), E-commerce Payment System and 99= USSD based payment system etc., are not in popular use therefore it is important to know the problems of digital payment system and its progress in India.

Objectives of Digital Payment Methods:-

The main objective of digital payment methods is to control the movement of illegal money from circulation in the economy, better tracking of transactions and ease of conducting online transactions, and increase transparency among monetary transactions among people.

Objectives:-

1. Improve the ease of conducting card/Digital transactions for an individual.
2. Reduce the risks and costs of handling cash at the individual level.
3. Reduce costs of managing cash in the economy.
4. Build a transactions history to enable improved credit access and financial inclusion.

Reduce tax avoidance.

Digital Payment Methods:-

1. **Banking Card**: banking sector provides various cards to avoid the time spend over the banking transaction. It offers consumers more security, convenience, and control than any other payment methods. There are many types of cards Rupay, master card, visa etc. they provides more security to the customer while using it. Payment cards give people the power to purchase items in stores on the Internet, through mail-order catalogues and over the telephone. They save both customers and merchants time and money, and thus enable them for ease of transaction.

2. **USSD**:- The innovative payment service *99# works on Unstructured Supplymentary Service Data (USSD) channel. This service allow to users mobile banking without internet. *99# facility available to make money transfer from one person to another without using internet and smart phones. *99# service has been launched take the banking services to every common man across the country. The Common number across all Telecom Service Providers on their mobile phone and can make transaction using an interactive menu on the mobile screen. Using this customer can check balance, transfer money, can get mini statements etc.

3. **Aadhar Enabled Payment System:** AEPS is a bank led model which allows online interoperable financial transaction at POS (Point of Scale or Micro ATM) through the Business Correspondent or Bank Mitra of any bank using the Aadhar authentication.

4. **UPI:** UPI is a Unified Payments Interface System that allow to multiple bank accounts into a single mobile application, merging several banking features. It is use to transfer money, received money, Bill payments and others. Now it is getting popularity among the Indian people. It is interesting and easy to use and not need to remember frequently use beneficiary's account number. The customer can get transactions history quick payment.

5. **Mobile Wallets**:-There are several mobile wallets are available and each bank have their own application. The customer can early digital cash through mobile wallet. By use of wallet customer can link credit card or debit card in mobile device to make transaction. An individual's account is required to be linked to the digital wallet to add the money. The Paytm, Freecharge, Mobikwik, Airtel Money, Jio Money, SBI Buddy, itz Cash, Vodafone M-pesa, Axis Bank Lime, ICICI Pockets, Speed Pay etc. the mobile wallets use in India.

6. **Point of Sales**:- A point of sale (PoS) is where sales are made. It allow to PoS holder to wallet money from their customer by the way of swap also and to need to go bank for making transaction of purchase and selling. On a micro level, retailers consider a PoS to be the area where a customer completes a transaction, such as a checkout counter. But it requiresGPS system internet and bank account of merchant.

7. **Internet Banking** :- Internet Banking, also known as online banking, e-banking or virtual banking is electronic payment systems that allow customers of a bank make transaction using website of the bank using ID and Password.

8. **National Electronic Fund Transfer (NEFT)**:- NEFT is a nationwide payment system which provides funds transfer from any bank any branch to any bank. Using the system individual firms and corporate can electronically transfer funds from any bank branch to any individual, firm or corporate having an account with any other bank branch in the country. Not only account holders but also without having account people cansent money to others account by depositing money from anywhere. However, such cash transaction have limit of Rs.50,000/- using this service individual can deposit money on Rs. 50,000/- and this facility can use in working days only.

9. **Real Time Gross Settlement (RTGS) :**RTGS is settlement of funds transfers individually on an order by order basis. 'Real Time' means the processing of instructions at the time they are received rather than at some later time. Considering that the funds settlement takes place in the books of the Reserve Bank of India, the payments are final and irrevocable. Transferring large amount RTGS is used. Customers can send minimum 2 lakh and maximum have no limit. RTGS can use in banking hours.

10. **Electronic Clearing System (ECS) :**ECS is an alternative method for the payment transactions like utility-bill-payments such as telephone bills, electricity bills, insurance premium, card payments and loan repayments, etc.

11. **Immediate Payment Service (IMPS)** : IMPS offers an instant, 24x7x365, interbank electronic fund transfer service through mobile phones. IMPS are a tool to transfer money instantly across India using mobile, internet and ATM it is safe and cost- effective.

12. **Mobile Banking**: Mobile Banking is a portable system provided by banks to customer on their mobile phones, smart phones with a special application using software. It provided by the banks or financial institution for the purpose. Each Bank provides its own mobile banking App for Android, Windows.

13. **Micro ATM**: Micro ATM meant to be a device that is used by the million Business Correspondents to deliver basic banking services. The micro ATM enables Business Correspondents to make instant transactions. It helps to withdrawals, transfers transaction instantly.

Advantages of Digital Payment System:

Time Server: Using digital payment system customer can pay to merchant transfer money quickly and no need to make payment by cheque and waiting for clearing. Because Digital Payment System take less time than traditional payment system take less time than traditional payment system.

Availabilities: Digital payment system can use by customer from anywhere and anytime there is no need to go banks for every transaction.

Easy Purchasing: The Digital payment system provides facility to user for purchasing by using ATM Card Credit Card and POS therefore it is easy for making transaction and no hard cash required to travel with us.

Use of Wallet: The Digital payment system includes digital wallets whichmake payment easy and with that wallet customer can get discount as well as cash back.

Written Record: You often forget to note down your cash spending. Or even if you note, it takes a lot of time. But you do not need to note your spending every time with digital payments. These are automatically recorded in your passbook or inside your E-Wallet app. This helps to maintain your record, track your spending and budget planning.

Less Risk: In Digital Payment System it provides us securities for every transaction it require MPIN or TP which can be avoid frauds in the system.

Barriers to Use Digital Payment:

1. **People use of currency note money:** In India people are using currency in High level. People in Rural area in India nearly made transaction 80% in cash. Because it is became traditional and habitual to the people.
2. **Computer Illiteracy:** There is only 6% people in India are computer literate and near about 90% Indian people don't understand the computer and internet that's why they cannot use the digital payment system.
3. **Use of ATM Card:** There are many digital payments systems but Indian people still using ATM cards for withdrawal and give money to other. They didn't use M. Wallet and digital payment for money transfer.
4. **Limited Availability of POS:** According to the reports of RBI there are 1.44 million POS terminals installed by banks across locations at the end of July 2016 and it increased by 24% in 2018. There should be involving every trader.
5. **Mobile Internet Penetrations Rate:** The use of mobile remains weak in rural India. For setting transaction digitally internet connection is requires but the connectivity are not available in the rural area.
6. **Risk and Security:** The Indian people still don't believe in online transaction. And they feel that the traditional system is good and faithful. And also not believe in Security of the transaction.
7. **Training:** There is a communication gap between bank and their customer. It requires giving training about use of online and payments system but banks do not provides any training program to increase the digitalization.
8. **Public Sector Banks:** There are 80% share of finance sector is occupied by public sector banks and the public sector banks started the digitalization from 1996. That's why it is in progressive trend. Private sector banks are ahead in digitalization to public sector banks.

Prospects:

1. The India banking sector is one of the best sector in India and it changes as per the requirementsof the India country.
2. There are large scope of digital payment system in India because of it increasing trend. The growth in volume and value of transactions using payment issued banks entities has been significant.
3. There are several banks and near about all banks are in adaption of Digital banking and NPCI also promoted Aadhar enable payment system to involve all Indian in digital transaction.
4. UPI system the best system to make digital transaction and it is expected to give a progress in digital payment transactions.
5. Debit and Credit card are shows as usual to make transaction but it is increasing trend from demonetization of money in 2016.

6. With increasing mobile banking services, growth in e-commerce and use of mobile payment applications, the use of cash will decrease.
7. RTGS and NEFT volumes increase almost threefold between 2013 and 2016 reflecting greater adoption of the system.
8. The Government of India is focus on digital infrastructure and it can encourage digital transactions culture in India there are almost every persons have Jan Dhan Yojana account and Aadhar Card.
9. As per the research there are 320 million above mobile users in India in 2018 and it is a good environment to motivate the Digital Payment System.

Conclusion:

Digital payment system is easy to use to the customer as well as bank officers and there are several option are available in the financial system in India, but there are large amount of people in India don't know how to use the system. The Digital literacy of Indian people is low level. Therefore Digital payment system is not pure developed and spread all over the India. The social and infrastructure barriers are there influences to use of digital payment system. But Now a day's mobile banking are becoming famous in the India because it is easy to use and anytime can use. It is also required to improve the digital literacy among the people. There are also issues relating to the risk and security.

- Crypto Currency = Digital Currency
- Money Laundering = Concealing, hiding (money obtained illegally)
- Tracking = Inquiry, monitoring
- GPS = Global Payment System
- MPIN = Mobile Banking Personal Identification Number
- OTP = One Time Password

References:-

1. https://www.researchgate.net
2. https://www.icommerececentral.com
3. https://www.indiajournals.com
4. https://www.cikitusi.com
5. https://www.inspirajournals.com

SOCIAL MEDIA – CYBER CRIMES

M. DURGA
Lecturer in Commerce,CRR College for Women, Eluru.

The Merriam-Webster dictionary defines cybercrime as "criminal activity committed using a computer, especially to illegally access, transmit or manipulate data." At its root, cybercrime is any illegal activity using a computer, either as the attacker's weapon or target. That covers a wide variety of types of crime, from phishing emails and identity theft that affect individuals, to ransomware and denial of service (DoS) attacks targeting businesses and organizations. There are also multiple categories of cybercrime offenders, from the hacker-in-a-hoodie stereotype to organized crime syndicates, cyberterrorists and nation-states.Cyber crime refers to any criminal activity that is perpetrated by means of a computer or internet. Common examples of cyber crime are email spamming, cyber bullying, identity theft, online child pornography, phishing and virus dissemination.

Social media refers to any digital tool that allows users to quickly create and share content with the public. It can be accessed through a computer, smartphone, iPad or any other device that has internet connection. Popular social networking websites include Facebook, WhatsApp, Twitter, Instagram and LinkedIn.Social media is a great platform for connecting with people, building relationships, sharing ideas and expanding businesses. Despite these great benefits, it is also a fertile ground for cyber criminals that are searching for unsuspecting victims.

The prevalence of the usage of social networking websites in today's digital age has also attracted internet fraudsters to set up multiple social media accounts and join many social media platforms so as to increase their chance of getting their victims.

In another academic study by Mike McGuire, senior lecturer in criminology at the University of Surrey, social media-enabled cybercrime is generating at least $3.25 billion in global revenue annually.

1. The prevalence of social networking websites usage has increased the number of cyber criminals worldwide.
2. The ability to communicate anonymously on social media makes it possible for most cyber criminals to be untraceable after defrauding unsuspecting victims.
3. It is very easy for cyber criminals to create fake identity on social media and use it to communicate with anyone around the world.
4. Malicious softwares and websites that look legitimate can easily be shared over social media with as many people as possible within a very short time.
5. Fake news which poses a threat to national or global security can easily be shared over the social media.
6. With the prevalence of the usage of social networking websites, online fraudsters can create as many social media accounts as possible with different identities and use it for criminal purposes.

7. Most sensitive information that are supposed to be private are now being shared publicly on social media. This of course increases the users' vulnerabilities.
8. Availability of many social networking websites makes it easier for cyber criminals to use their multiple social media accounts to send fraudulent and unsolicited messages to unsuspecting victims.
9. Proliferation of social networking websites has also contributed to the increase in cyber terrorism.
10. The criminal community on the dark web where cyber criminals buy and sell stolen sensitive information is getting bigger because the social media platform has become a fertile ground for online scammers.

CYBERCRIME TYPES

The types of cybercrime continue to grow and evolve as new channels of digital communication develop. Here are broad varieties:

1.PHISHING-Perhaps the "original" email scam, phishing is when fraudsters spam users online with emails promising prizes or threatening an account suspension, for example, then asking them to click on a link or go to a site to sort things out. Instead of winning a gift or reactivating that frozen credit card, users instead get their identities stolen or their computers infected with viruses. Phishing remains the most popular form of cyberattack, and it has endured despite all efforts to fight it off. In recent years, phishing has evolved in new directions, such as targeted spear phishing, smishing (via text message) or vishing (using voicemail).

2.IDENTIFYING THEFT : Just as it sounds, identity theft involves stealing personal information to use for fraudulent purposes. Cybercriminals can attack individuals through phishing scams or break into corporate systems and steal databases of sensitive information such as credit card or Social Security numbers. Entire catalogues of information are up for sale on the Dark Web, where fraudsters acquire them for their various exploits.

3.RANSOMWARE: Cybercriminals have developed the highly profitable tactic of breaking into databases, extracting and deleting files, or encrypting them so the organization they belong to can't get access. The attackers then extort payments usually in cryptocurrency in exchange for returning or unlocking compromised data. This practice has grown into a veritable ransomware crime wave in 2021.

4.DENIAL OF SERVICES (DOS): In the traditional DoS version, attackers flood a service or computer network with requests. This overwhelms the website's servers, causing them to crash and taking the site offline. Another version of this type of cybercrime, distributed denial of service (DDoS), uses multiple attackers in different geographical locations to swamp the network from different IP addresses and make it harder to fight off the attack.

5.MALWARE ATTACKS: Ransomware is one type of malware attack, but malicious software comes in many varieties, all designed to infiltrate a computer system and perform an unscrupulous activity on behalf of a cybercriminal. Spyware, just as its name implies, records activity without the user's knowledge, while keyloggers record each keystroke users make on their keyboard. Rootkits can give a hacker control of a user's device, such as a webcam. Malware sneaks into systems in many ways.

6.CYBERSTALKING: This is the digital evolution of the "analog" crime. In this case, a stalker tracks the victim online, gleans information from online sources and communicates via digital channels, harassing and threatening the victim. Some cyberstalkers use spyware and gain access to webcams and digital speakers in order to stalk their victims. Some cyberstalking escalates to a form of blackmail where the criminal uses photos or videos of the victim to extort money . The FBI has

recently become more concerned about this particular crime after seeing a spike among young people.

7.**WEBJACKING AND BRAND EXPLOITATION:** In webjacking, criminals don't steal something from a website, they take the whole site, or the traffic meant for it. This is usually done by gaining administrator access through fraudulent means and tampering with the Domain Name System (DNS) to bring users to a criminal site.

How to identify if the profiles are genuine or fake?

- A fake profile on Facebook will not use their genuine pictures (Having said this there are people who takes photographs of other genuine people as their profiles are public and use it to create a fake profile)
- They don't have many friends.
- Even if you make someone your friend, try to scroll their profile to check their status updates and their experiences they share, if there are not any – they are more likely to be fake.

Tips how to be safe from Information Theft:

- If you have a name which is common differentiate it with something that people know would connect to your business.
- Ensure that you get the right SEO and report your business page through Facebook India.
- It is possible to merge pages on Facebook, so you can merge the fake page with yours and claim that you are the official owner of the page.
- Ensure that you don't store credit card details and crucial passwords on Social Media messengers too.
- When you use email extensions on chrome, beware they are genuine one as they are reading through your emails and have access to all the data.

Conclusion:

However, social media is also an effective tool for combating cyber crime because many people can easily take picture or record video of cyber criminals while they are committing cyber crime. The picture and recorded video can be shared with many anti-graft agencies and law enforcement agents within few minutes. This of course will help a lot in the investigation and prosecution of the cyber criminals.

DIGITAL EDUCATION – GOVERNMENT INITIATIVES

J. DEVA MANI
Lecturer, SIR C R Reddy College for Women, Eluru.

INTRODUCTION

Digital education is the innovative incorporation of modern technology and digital tools to assist the progress of teaching and learning. It is also known as Technology Enhanced Learning (TEL), digital learning, or e-learning. Digital education is the way forward to seeking education through the means of technology and digital devices.

A Brief Overview:

Digital transformation of the country is underway and digital evolution of the economy and society is possible only through digital education. The concept of digital learning is not new and has existed in various forms for many years now, but when the COVID-19 pandemic suspended face-to-face teaching its significance increased manifold. Most educational institutions are adopting digital education as a solution while traditional classroom setup takes a back seat for some time due to the currently prevailing pandemic. Digital education is being seen as an alternative to the traditional education process of chalk and talk.

The emergence of the internet and ever-evolving technology has made learning interactive, engaging, motivating, and handy. Education is not anymore limited to textbooks and classrooms; it has become an amalgamation of technology, innovative learning, and digital content. The internet has become far more affordable and accessible and this shall lead to a greater confluence of digital and traditional teaching methods. The government is actively involved in taking essential steps to come forward with policies that will boost the digital education market in India. The efforts are being made to uplift the standard of digital infrastructure pan India to help facilitate the utilization of innovative educational tools. In near future, digital education like all other sectors will witness noticeable amendments in the way educational institutions function.

Ministry of Human Resources Development (MHRD) – Initiatives for Digital Education

A comprehensive initiative called PM E Vidya was announced on May 17, 2020, which aims to unify all efforts related to digital/online/on-air education to enable equitable multi-mode access to education. It is envisaged that it will benefit nearly 25 crore school going children across the country. One of the most important initiatives of MHRD is DIKSHA (Digital Infrastructure for Knowledge Sharing).

1. DIKSHA (Digital Infrastructure for Knowledge Sharing): As part of PM E Vidya announced under the Atma Nirbhar Bharat programme, DIKSHA is the 'one nation; one digital platform' for school education in India. It was launched in 2017.It is a national platform available for schools in all states. DIKSHA is available for grades from 1 to 12.DIKSHA can be accessed through mobile application and web portal.

2. VidyaDaan - It was launched in April, 2020.It is a content contribution program at national level, that makes use of the DIKSHA platform and tools, it allows donation or contribution of e-learning resources for school education by experts, private bodies, and educational bodies.

3.Swayam Prabha – TV Channels -This mode of education is for people who do not have access to education. High quality educational programmes are telecasted. There are a total of 32 channels to meet the requirements. Different channels are used for higher education and school education. The Department of School Education and Literacy also tied up with private DTH operators like Tata Sky

& Airtel to air educational video content to enhance the reach of these channels. Number of TV channels for school education will increase from 5 to 12 to transform into 'one class, one channel', that is, one channel each for all grades from 1 to 12 channels. To ensure asynchronous usage at any time, anywhere, and by anyone, the same content will be organised by chapter & topics on DIKSHA.

4.E-textbooks- e-Pathshala mobile app (Android, iOS, Windows), and web portal can be used to access e-textbooks. It can be accessed by students, teachers and parents. 3,500 pieces of audio and video content of NCERT are available. It is available in different languages – English, Sanskrit, Urdu, Hindi. For the differently-abled For hearing impaired students, one DTH channel is available with sign languages. Study material has been developed in Digitally Accessible Information System (DAISY), for hearing and visually impaired.

5. Radio Broadcasting - The radio broadcasts focus on activity-based-learning.For broadcasting content related to National Institute of Open Learning NIOS (grades 9 to 12), 289 community radio stations have been used. This mode of education is particularly useful for students who are living in remote areas, particularly for grades 5 to 1.Shiksha Vani is a Podcast of the Central Board for Secondary Education (CBSE)

6. SWAYAM – Under the digital India ,one of the thrust area is Massive Online Open Courses. MHRD, government of India has embarked on a major initiative called " Study Webs of Active Learning for Young Aspiring Minds" to provide an integrated platform and portal for online.

7. E-Yantra: It is an initiative to spread education in Embedded systems and Robotics by IIT ombay sponsored by MHRD through the National Mission on Education through ICT.

Digital Education in India – Way Forward

Developing quality e-content in local languages, to address the diversity of Indian languages. Addition of skill development courses, virtual labs, virtual vocational training. Framing of Online/Digital Education Guidelines addressing the digital divide. Developing digital classrooms by integrating education systems and technology. Developing framework for assessments in the era of digital education. Making sure of coherent user experience by multi-mode access to education through Mobile apps, web portals, TV channels, radio, podcasts. To enable "anytime, anywhere" access and increase penetration, focus will be on increasing usage of mobile phones. Priority for providing complete access to anytime, anywhere e-content and e-infrastructure is for all learners in schools; however, e-content is being developed with slightly varied priorities – Grades 12 to 9 covering 6.3 crore children will be the top most priority. The next in the table of priority will be from grades 8 to 6 covering students strength of 6.4 crore children. For grades 5 to 1, the priority will be on numeracy and foundational literacy.

Advantages of Digital Education in India

1. 1.This initiative has made students not just gain bookish information but also gain practical and technical knowledge
2. 2.No limitation as to the place of learning or studying. With digital learning, a student can engage in online classes or learning anywhere, at any time
3. 3.With study material available online, students can take their time to understand any topic
4. 4.Through the mode of digital education, learning can be made more engaging and interactive between the students and teachers
5. 5.It is also important that Digital Education acts as a supplement and does not completely overpower physical education.

Challenges with Digital Education in India

1. A lot of technology-based adaptations will have to be encountered by the Government to ensure that digital education can be reached out to students across the country.

2. Availability of internet connection to all is one of the biggest requirements for digital education. This will have to be achieved by the Government for easy access to information
3. Providing the devices and technology to the people belonging from socio-economically weak sections so that they are not deprived of education
4. Training teachers is another challenge. Only when the teachers are technically sound, they can conduct the digital classes
5. Making digital cost-effective should be a key motive of the Government
6. To ensure that Government schools and colleges are provided with proper facilities for digital classrooms.

References

https://www.jirs.ac.in
https://www.ibef.org
https://www.researchgate.net
https://teachmint.net

SOCIAL MEDIA & ONLINE CRIMES

S. ANURADHA
Lecturer ,CR Reddy College,Vatluru

Social media is a term used for technology that focuses on communication, interacting with others information among friends, employees, families etc. Facebook, Youtube, Whatsapp, Instagram etc are few examples of social media.

There are different forms of social media like blogs, micro-blogs, wikis, social networking sites, photo-sharing sites, video chattings, conference calls etc.

History : 'Six Degrees' is the first recognizable social media site created in 1997 by Andrew Weinreich called 'Father of social Networking'. The first blogging sites became popular in 1999. Social media gained prominence in the early 2000's.

Types of Social Media:

1. Social networks: Used to share information, thoughts and ideas.
   Ex:- Facebook, Linkedin.

2. Media-sharing networks: Used to share content, videos etc.
   a. Ex:- YouTube, Instagram.

3. Community- Based networks: Used for in depth-discussion mostly in blog form.
   a. Ex:- Reddit.

4. Review board networks : Used for product review or service review.
   Ex:- Yelp.

Life seems to be impossible now-a-days without social media. There are several benefits of using social media.

- Major source of information sharing.
- Relationship building
- Educating oneself
- Entertainment
- Timepass
- Awareness
- Excelling in arts
- Hobbies
- Product marketing
- Brand promotion
- Problem solving
- Crowdsourcing
- Recruitments
- Audience building

- Fashion updates

Disadvantages : Increased usage leads to Cyberbullying, social anxiety, depression and exposure to content that is not age appropriate.

- Addition
- Cyber crimes
- Psychology problems
- Eye and Brain damage
- Kills time
- Fear of missing out
- Self image issues
- Bullying
- Suicidal tendency
- Dissemination of fake news

Cyber crimes : Crimes by using electronic devices for stealing someone's data or for harming someone are called cybercrimes. Due to advancement in technology and accessibility to the internet, there is much scope for everyone to reach it and open the path for cybercrimes. High speed internet has shortened the data transfer time which made cyber crimes much easier.

Types : Cyber crimes can be classified into 4 major types

Financial crimes: Stealing lots of money from public, private and government sectors. It is of great loss.

Privacy related crimes: Stealing of personal data. It is of great threat to the Victims, related with emotions and feelings of the people especially ladies.

Hacking : Involves defacing a website to intentionally or making changes in the existing websites to decrease its value.

Cyber terrorism : It is not only restricted to terrorist activities but also involves threatening people or properties.

Effects of Cyber crime : Financial Loss
Drop in the value of business
Loss of sensitive customer data
Increased need for cyber security
Increased premium costs

Laws related to cyber crimes: Cyber crimes are increasing day by day. There is an immense need to resolve them. It is estimated that nearly rs1.25 lakh crore/annum is lost by the Indian government due to cyber-attacks.

In order to stop the spread of cyber crimes and to protect the public, government has made several laws in every field.

Cyber Law is a legal system that deals with the internet, computer systems, cyber space and all matters related to cyberspace or IT.

Information Technology Act (2000) : It is the first cyber law to be approved by the Indian parliament. Its main objective is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication.

Indian Penal code, 1860: It implies when the IT Act is not sufficient to cover specific cyber crimes.

Companies Act, 2013: It is the most pertinent legal obligation to properly manage daily operations.

Cyber Security Framework (NCFS) : It aims at fostering resilience and protecting critical infrastructure.

Cyber crime reporting portal : It is an initiative of the Indian Government to file complaints online. This portal focuses on cyber crimes against women and children. These complaints are dealt with by law enforcement agencies. Correct information has to be provided while filing complaints.

Prevention of Cyber crimes : Backing up of data, systems etc
Enforcing and checking security settings.
Avoid sharing of personal information to strangers
Usage of antivirus software.
Restricting the access of most valuable data.

Cyber Security : It is a domain that is designed to eliminate cyber crime. It is also referred to as IT security. It is the backbone of network and information security. Cyber security gives in-depth knowledge about how to control or recover from cyber attacks.

Conclusion: India was the country with the highest number of cyber crimes in 2020, amounting to 4.5million. Social media is like a double-edged knife. The way we use it depicts its greatness. It has both advantages and disadvantages. Cybersecurity provides a thorough understanding of how to control cyber crimes.

51

CYBER CRIME -TECHNOLOGICAL CURSE

Dr. Ch. SWAPNA
Lecturer in Zoology,Sir C.R.R. College for women,Eluru.

What is Cyber Crime

Cyber Crime is the term used to define criminal activity in which computer networks are a tool, a target or a place of criminal activity and it includes everything from electronic working to service attacks .It covers crimes like Credit card frauds, Bank robbery, illegal downloading, Industrial espionage, Child Pornography, Kidnapping children through chat rooms, Scams, Cyber terrorism, oration and or distribution of viruses, spam and so on. Traditional crimes are also covered in this cyber crime, in which computers or networks are used to enable the illicit activity. Now a day, it has become a new fashion to earn money by fraud calls or to take revenge through hacking of her accounts .However the opportunity for cyber criminals to find and exploit soft targets has increased with the switch to working online. Now, the Indian Government must get up to speed and improve cyber security overall.

Cyber crime is the criminal act which takes place over the internet through computers as tools or targets or other smart devices meant for making our work easier. The hacker or criminals are having various motives of the crime. They may be involved to cause a loss to an individual, some organization or government. Several examples of cyber crime include frauds, identity theft, cybers talking, creating and sending malware like viruses for destroying the systems or steal the data to make money. People involved in such activities find them as an easy way of making money. Even many of the well-educated and knowledge full persons are involved in such activities. Instead of using their mind in a positive way they employ themselves in cyber crime activities. Day by day this is becoming a great threat to our society and nation.

Why is cyber security important

No one can imagine that someone will use their personal data to s teal from them. And that is what cyber crime is in theft. For example financial cyber crimes can s teal money directly. Cyber crime scandal so include industrial espionage, where cyber criminals steal ideas, patents and even customers. Good cyber security measures and secures your information .They could also make it costly for cybercriminals to access you're in formation .Now a days thankfully it is easy to establish a good cyber security system, whether you are tech savvy or not.

Common types of hacks and Malware

Phishing Attacks:-

Phishing involves using thrust worthy emails or web pages to scam people by clicking the link or providing their personal information your money or identity is stolen by cyber criminals by successful phishing attacks. The success rate of phishing attacks is incredibly low with current security soft ware and knowledge, but some attackers reach their target.

Vising Attack:-

It is considerable as a type of a social engineering attack, where they are performed over the phone.

How Vising works:-

Common tactic is the use of authority .For instance the attacker may pretend to be from the IRS pretending to be calling to collect unpaid taxes. The fear of arrest can cause victims to do what

the attackers tells them to do. Then types of attackers also commonly involve payment via gift card, have cost victims.

What is the difference between Vishing and Phishing

Both Vishing and Phishing are social engineering attacks and same tactics are used, the main difference between them is the medium used to perform the attacks. Vishing uses the phone for an attack Phishers on the other hand, use electronic ,text based forms of communication to perform their attacks, while email is the most common and well known phishing medium, attackers will also use text messages called smishing, corporate communication apps like Telegram signal, Whatsapp etc., or Social media like Face book ,Instagram etc., to perform their attacks.

Types of Cyber Crimes:

Crimes against persons are:-

Cyber stalking:- It means to create physical threat that creates fear to use computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

Deformation:-It is an act of imputing any person to lower down the dignity of the person by hacking is mail account and sending mails vulgar language to unknown persons mail account.

Hacking:- It means unauthorized control or access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers hacks mobile network and telecommunication.

Carding:-It means false ATM cards i.e. credit and debit cards used by criminals from the victims back account.

Child pornography:- It involves the use of computer networks to create, distribute, or access materials that sexually exploit under age children.

Cyber crimes against Government

Cyber Terrorism:- Cyber terrorism is a major burning issue in the domestic as well as global. The common form of terrorist attacks on the internet is by distributed denial of service attacks, hate websites and hate e-emails, attacks on sensitive computer networks etc.

Distribution of Pirated software:- It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.

Crimes against property:

Intellectual property crimes:- Intellectual property crime in committed when some one manufactures sells or distributes counterfeit or pirated goods, such as patents, trademarks, industrial designs or literary and artistic works, for commercial gain

Hacking computer systems:-Hacktivism attacks there included famous twitter, blogging platform by unauthorized access or control over the computer, there will be loss of data as well as computer.

Transmitting virus:- viruses are programs that attack themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it.

Impacts of Cyber Crime

Cyber crime has ruined up the lives of many. The people involved in cyber crime are called hackers. If we discuss on an individual level, the people affected with this are still trying to adjust the loss. Some have opted to commit suicide. The ultimate loss of money and any data which is confidential make the person helpless and left out in a painful situation.

On an organization level, the loss is made by stealing the data of the company or destroying the system by malware so that it may not work till the terms and conditions of the criminal get

fulfilled. The companies are at a greater loss as their strategies and important data is stolen and leaked out.

The government is also the victim of this offence. Much confidential data is leaked as the result of cyber crime at the government level, risking the nation's sovereignty. This is a serious issue as it may happen that the lives of people of the nation are threatened and frightened. The loss can be economical too. Many lakh and crore have been lost from the nation because of these cyber crimes.

Need For Cyber Law

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.In today's highly digitalized world, almost everyone is affected by cyber law.

For example:

Almost all transactions in shares are in demat form.

Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.

Cyber Laws In India

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

The existing laws of India, even with the most compassionate and liberal interpretation could not be interpreted in the light of the emergency cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgement found that it shall not be without major threats and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence, the need for enactment of relevant cyber laws.

None of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email id not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyber law.

World and Cyber Laws

- The Great firewall of China monitors every moment in cyber space and protect to publish any offensive content.
- China have an hold on every content which is harmful of dangerous for the government of China.
- Brazil is considered world's biggest airport for Hackers.
- Iran is also a dangerous country for the Netizens. He also have a Crime Police unit for crime in Cyber Space.

Importance of Cyber Laws

- We are living in highly digitalized world.

- All companies depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication.
- Even in "non-cyber crime" cases, important evidence is found in computers/ cell phones e.g. in cases of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.
- Since it touches all the aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace therefore Cyber law is extremely important.

Conclusion

Cybercrime is the most prevailing crime in the present scenario, done through internet. It causes a severe loss to the victim. Therefore some of the measures should be taken by us to avoid such crimes. The vigilant behavior and following the safety protocols are only helping aids which can reduce the occurrence of cybercrime. The IT Act and the Rules promulgated there under regulate the cyber law regime. When the IT Act is unable to provide for any specific sort of offence or if it does not include exhaustive provisions with regard to an offence, one may also turn to the provisions of the Indian Penal Code, 1860. However, the current cyber law system is still insufficient to cope with the wide range of cybercrimes that exist. With the country advancing towards the 'Digital India' movement, cybercrime is continuously developing, and new types of cybercrime are being added to the cyber law regime on a daily basis. So, there is a need to bring some amendments to the laws to reduce such crimes.

58

SOCIAL MEDIA ONLINE CRIMES BY GRAPH THEORY

Ms. EDUBILLI TEJA DEVI SOWJANYA M.Sc.Math's,
Lecturer in Mathematics, SIR C.R. Reddy College for Women, Eluru.A.P.

ABSTRACT

Since a past decade, social media networking has become an important part of everyone's life affecting cultural, economic and social lifetime of the people. These social networking sites are attracting users from all walks of life and keeping these users' data within the cloud. Today's big challenge is said to an increase in volume, velocity, variety and veracity of knowledge in social media networking, and this results in creating several concerns, including privacy and security; on the opposite hand, it also proves as a tool to stop and investigate cybercrime, if intelligently and smartly handled. Consistent with internetlivestats.com, in March 2019 the web users reached 4 168 461 500, i.e., 50.08 penetration of world population. Consistent with Statistics, in 2019 there are 2.22 billion social media networking users worldwide, i.e., 31 you look after global social media networking penetration and it is expected that in 2021 this number will reach 3.02 billion. A graph is formed up of nodes; just like that a social media is a kind of a social network, where everyone or organization represents a node. These nodes during a social media are interdependent on each other via common interests, relations, mutual friends, knowledge, common dislikes, beliefs etc. the general graphical structure of a social media can be very complex with millions of nodes and thousands of interconnections amongst them based upon various grounds. Many researchers have revealed that social network works on various levels and helps in understanding many things like how an entire organization is run. It helps to unravel and understand many critical problems.

Key words: *Cybercrime, Cyber Security, Social Media, Graph theory, Graphical Structure.*

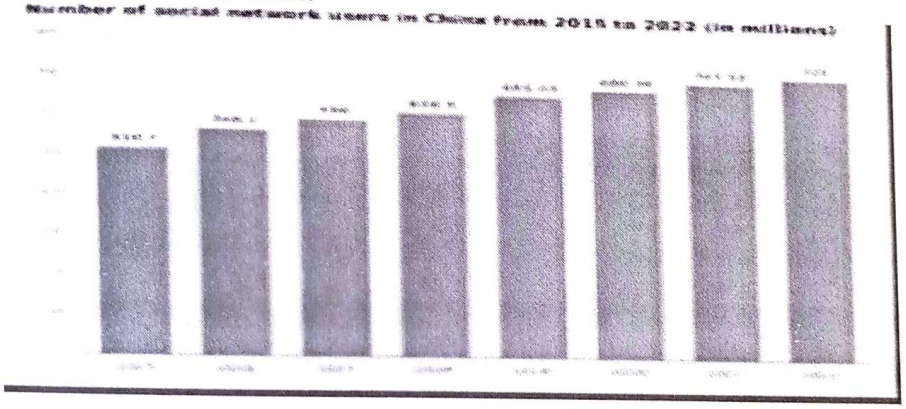
INTRODUCTION:

Social media affects cultural, economic and social lifetime of the people, and it's become an essential part of everyone's life. Social media networking may be a platform that enables users to participate and share multimedia content, for instance, text, audio, video, images, graphs and animations through a medium of an internet site or an application. These contents are cloud-based big data contents and may be viewed in the form of volume, variety, velocity, veracity, volatility, quality, discovery and dogmatism. Nowadays, a world without the web is inconceivable. We Are Social (2019) reports that the amount of internet users around the world is continuously growing at a remarkable rate, with approximately 900,000 people logging on for the first time every day since July 2018. The year before that, 46.8% of the worldwide population accessed the internet, which is predicted to grow to 53.7% in 2021.These users are of various age group, different cultures, different religions, different social attitude, behaviors, and that they use different devices to connect to the social media sites. Keeping in sight the popularity of these networking sites, users of all types are attracted to these social media sites to meet friends and family, to share their daily routine with the loved ones and find new acquaintances. Roughly six out of each ten of the entire world's population currently have internet access (Oberlo, 2019). The amount of internet users in 2019 marks a 327 million year-over-year increase compared to Q3 figures of 2018. this means 8.2% growth within the active internet users across the globe, which is over eight times faster than the entire population growth, which stands at 1% (Oberlo, 2019).These social networking sites are attracting users

from all walks of life and keeping these users data within the cloud. The way we started living within the online world today is changing the way regarding our privacy and security. Graph theory may be a mathematical concept which is based on mathematical structures made up of nodes and edges, called 'graphs', which are wont to model pair-wise relations between objects. a web social network (OSN); which is used by people to build social networks or social relations with other people can be represented by a graph with nodes and edges and analyzed in order to determine many graph theory properties associated with them. It is certain that human behavior plays a vital role in many fields such as management, marketing, trading, politics etc. together with the advancement of information and communication technology, predicting human behavior and their requirements has been a challenging task. As OSNs become the tools of choice for connecting people, sociologists expect that their structure will increasingly mirror real world society and relationships. This has been proven mainly by comparing the power law distribution and small-world property of real-world social network thereupon of OSN. Therefore, Graph theory concepts provide an efficient and efficient method to analyze and evaluate OSNs which will provide a strong base of information to determine and predict human behavior in the network.

SOCIAL MEDIA USERS:

Social media has been on rise in past several years, which changes the communicational landscape. Social media sites, such as Face book, Twitter, and YouTube, have millions of active users. Using these websites, people communicate instantaneously with each other with convenience. Social media sites are used by people to communicate with each other, and by the public sector for advertisement and recruitment of new employees. Statista's data on social media users as 2015 TO 2022.



Robbery via Social network:

Here criminals search social media for a possible target for burglary. Social media users usually post their personal activities, for instance, they're having dinner or going somewhere for vacations. Criminals search for this type of information to find easy targets, where they find large time-frame to burgle the property [9]. Consistent with BBC report, robbery of 10 million USD worth jewelers from different last year is that the prominent example of this type of crime.

EMAIL PHISHING:

An example of a phishing email, disguised as a politician email from a (fictional) bank. The sender is attempting to trick the recipient into revealing tip by "confirming" it at the

phisher's website. People using social networking sites receive messages from their friends requesting immediate financial assistance. Actually, these messages weren't sent by their friends, but by the criminal who stole their friends' emails and passwords. Cybercriminals make use of varied methods to get potential target information by social engineering tricks and tactics. Phishing emails might appear as if from the boss asking employees login credentials or from the bank of the individual. Cybercriminals ensure of making their target scared so that they do as instructed rather than think rationally. Criminal using this system sends millions of emails in hope of receiving useful information. The foremost common form of phishing is to make a Facebook or Bank like page.

GRAPH THEORY AND SOCIAL MEDIA:

The concept of graph theory is extensively utilized in social media. Usually here the users or the people involved are considered because the nodes or vertices. And any relation between the users thanks to common likes or mutual friendship is considered as edges.

Graph Theory in Facebook: Majority are conversant in Face book these days. you'll click 'like' if you find something likeable, 'tag' your friends in various 'posts', put comments in posts and most significantly befriend someone whom you know and also someone whom you don't know! The concept of graph theory is used in Face book with each person as nodes and every like, share, comment, tag as edges.

Graph Theory in Twitter: Here the persons are considered as nodes and if one person follows another then that's considered as the edge between the two

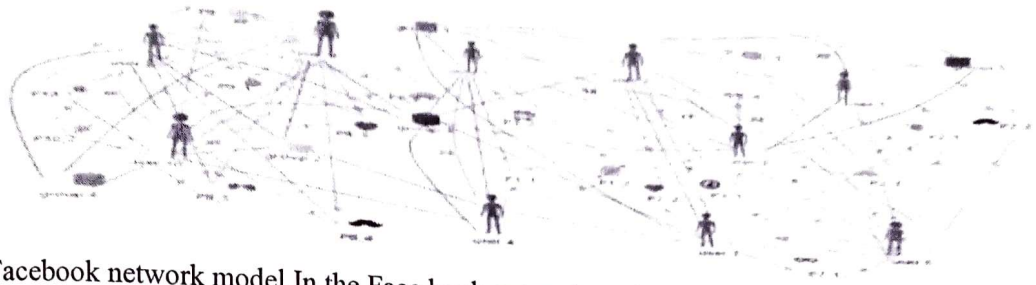
Brief idea on Social Network:

When we need to represent any form of relations in the society in the form of links, it is often termed as Social Network. The pattern of interdependency between each individual (node) are often based on different aspects, viz. - friendship, interconnection between families, common interest, financial exchange, dislike, sexual relationships, or relationships f beliefs, knowledge or prestige.

CONSTRUCTING OF GRAPH MODELS:

There are several activities inherited to on-line platforms of Face book, Twitter and LinkedIn. The users may create new bonds with other users, they may post their photos on on-line platform so that their friends can see them, or they may send messages to their friends etc. The way in which these activities are carried out may vary with one network to another. So,

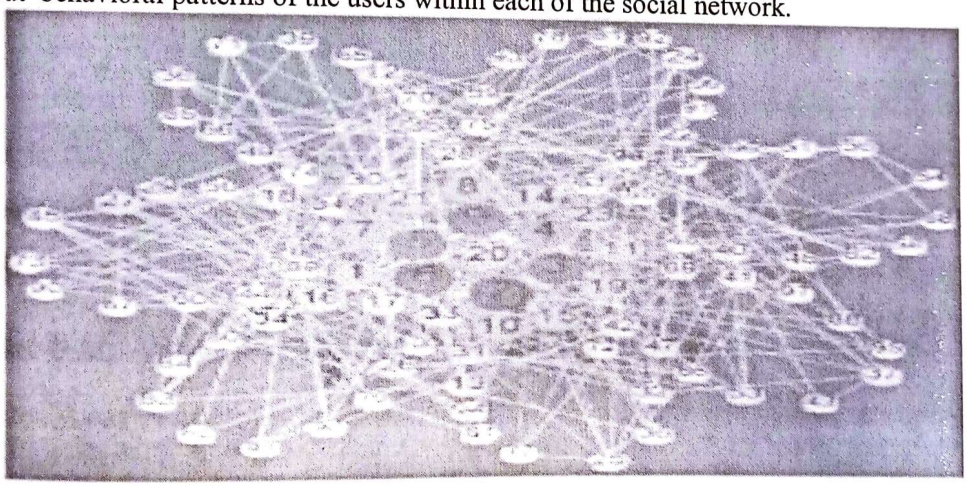
determining each activity in the three sites is essential in order to model the social network of each of the social media site. Model of a social network describes a graph with several types of nodes and edges with respect to each activity on the online platform. According to each model, many sub graphs can be extracted and analyzed in order to predict behavioral patterns of the users within the network. The constructed models of social networks of Face book, Twitter and LinkedIn



Facebook network model In the Face book network model, there are three types of nodes which are users, posts and groups. The links are friendship (red), reactions on posts (green), creation of posts (blue), messages (pink) and group membership (purple). Four sub graphs can be extracted from Face book network model to analyze the user behavior of Face book. They are; Friendship graph, Graph for reacting on posts, Groups graph, Messaging graph.

ANALYSIS:

Online social networks of samples of users of Facebook, Twitter and LinkedIn are generated by using the software, Gephi. The graphs are generated using Barabsi-Albert network construction method. It's a MATLAB code which produces an adjacency matrix to represent a network. Barabsi-Albert algorithm has been specifically written to get scale-free networks. Just one graph is constructed if there are common sub graphs in the three models of Face book, Twitter and LinkedIn. Then, graph theory properties of the constructed graphs are analyzed to work out behavioral patterns of the users within each of the social network.



CONCLUSION:

By taking the examples of social media and graph theory how the users are used frequently in face book and twitter and different platforms. Various activities of Face book,

Twitter and LinkedIn can be identified and a suitable graph model for each social media to represent respective activities can be constructed. It is possible to evaluate graph theory properties of the constructed models of each social media separately in order to analyze behavioral patterns and characteristics of the users.

REFERENCES:

1. N. Thabet and T. R. Soomro, "Big Data Challenges," *Journal of Computer Engineering & Information Technology,* vol. 4, no. 3, 2015. https://doi.org/10.4172/2324-9307.1000133
2. Internetlivestats.com, "Internet Users," Internet Live Stats, 2019.
3. S. Inc., "Number of social media users worldwide from 2010 to 2021 (in billions)," Statista: The Statistics Portal, New York, 2019.
4. T. R. Soomro and H. Wahba, "Perspectives of Cloud Computing: An Overview," *Proceedings 14th International Business Information Management Association (IBIMA) Conference on Global Business Transformation through Innovation and Knowledge Management*, Istanbul, 2010.
5. NW3C, "Criminal Use of Social Media (2013)," NW3C, 2013.
6. M. Sauter, "Nine Major Ways Criminals Use Face book," Fox Business, 2012. [7] Symantec, "What is social engineering?," Symantec Corporation, 2015.

CYBER SECURITY IN OUR ECONOMY-- DIGITAL PAYMENT & CYBER THREATS

**K.V,V. SRINIVAS
Sir C. R. Reddy College for Women, Eluru,

**Dr SHAMEENA BEGUM
Ramachandra College of Engineering, Eluru

ABSTRACT

The article provides a brief report on the various digital payment methods that has emerged and evolved through out the period in India as part of the 'Digital India' programme launched by the Government of India to promote Cashless transactions in the Indian Society as a scope to prevent the unaccounted economy such as 'Black money'. In parallel to the developing trend of digital transactions, the threats and vulnerabilities in this Cyber domain has increased rapidly. Digital payment gateways are one of the fastest and greatest methods for transaction of huge amount of money whether they are personal or business transactions without any physical vulnerabilities. However, this requires large databases with high level security architectures such as PCI DSS Compliance, Secure Socket Layer(SSL), Secure Electronic Transaction(SET) and other data encryption techniqueswhich constantly provides authorized payment gateway checks and prevents any type of masquerador attacks (system access for unauthorized users). Recent statistics have concluded that the digital payment gateways are one of the fastest and greatest methods to stop corruption in the Indian Economy. Through the cyber security techniques we can secure our money it is necessary to know every citizen.

Introduction

Payments are made using payment instruments. Check and cash are examples of payment instruments. However, digital payment is not a single instrument but rather an umbrella term that is applied to many instruments used in various ways. It can be defined as a way of paying for services or goods via an electronic medium without the use of cash or check. It is also known as electronic payment system or e-payment.

History

When Point Of Sale (POS) terminals made their way into the Indian financial ecosystem in a full-fledged manner in 2016, there were challenges that simultaneously struck the nation in terms of their full acceptance. Nearly a decade ago, people in India hesitated to even indulge in online transactions as they found cash to be the only trustworthy and secure way to make payments. While e-banking has been there in the Indian spectrum since early 2000s, it was limited to big business transactions.

India adapted to the transition of paying via digital means almost overnight. Post demonetisation, digital transactions found their way into the Indian psyche. Immediately afterwards, government began providing people with several incentives or concessions or benefits for opting to use online methods of making payments. Ever since payment gateways and APIs (Applications) came into existence, they have proven to be a boon for the economy since these platforms does not require physical presence of cards.

DIGITAL PAYMENT METHODS

1.Banking cards

Cards are one of the most extensively used digital payment methods, offering a variety of features and benefits such as payment security, convenience, and so on. Customers can keep card information in digital payment apps or mobile wallets to make a cashless payment. Among others, Visa, Rupay, and MasterCard are some of the most reputable and well-known card payment systems. Banking cards can be used for online shopping, digital payment apps, point-of-sale machines, and internet transactions, among other things.[1]

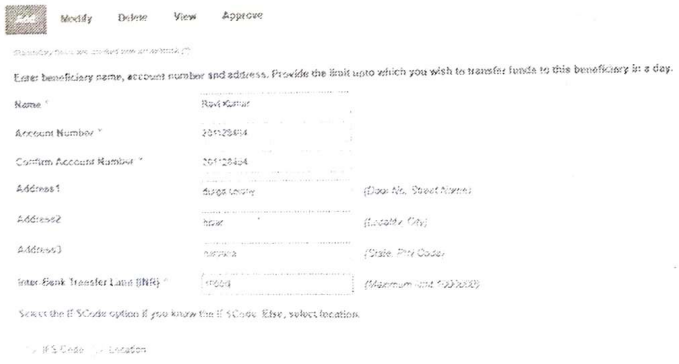
2. Point of sale(POS)

An important component of a point of purchase is the location where a client makes a payment for goods or services and where sales taxes may be due. It could be a physical store with PoS terminals and systems processing card payments or a virtual sales point like a computer or mobile electronic device. The merchant may utilize various technologies such as weighing scales, barcode scanners, and cash registers to calculate the amount due by a consumer (or the more advanced "POS cash registers", which are sometimes also called "POS systems).

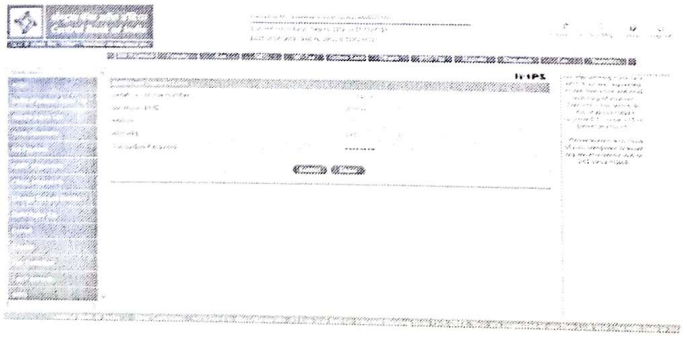
3. Internet banking

There are different services included in internet banking such as account balance check, view bank account statements, NEFT & RTGS Funds Transfer, IMPS Fund Transfer, issuance of cheque book and many other services as well. Funds can be transferred through internet banking by three methods namely NEFT, RTGS and IMPS.

NEFT



RTGs



4. USSD

Another digital payment technique is by dialling *99#, which can be used to make mobile payments without downloading an app. These forms of payments can be done even if you don't have access to mobile data or the internet. The USSD and the National Payments Corporation of India (NPCI) support this service.[2]

5. AEPS

AEPS can be utilised for various banking operations, including balance inquiries, cash withdrawals, cash deposits, payment transactions, and Aadhaar to Aadhaar fund transfers, among others. Based on Aadhaar verification, all transactions are processed through a banking correspondent. There is no need to go to a branch, produce debit or credit cards, or even sign a paper in person. Only if your Aadhaar number is registered with the bank where you have an account can you use this service. The NPCI has taken another step to promote digital payments in the country through AEPS.

6. UPI

UPI is an interoperable digital payment system that allows any consumer with a bank account to send and receive money via a UPI-enabled app. The service allows users to link multiple bank accounts to a UPI app on their smartphone, allowing them to seamlessly conduct financial transfers and collect requests 24 hours a day, 365 days a year. UPI's key benefit allows users to send money without a bank account or an IFSC number.

All you'll need is a Virtual Payment Address to get started (VPA). There are no fees associated with using UPI. Some of the examples of UPI enabled apps include PhonePe, Paytm, Bhim App, Google Pay, Google Tez, MobiKwik etc.

7. Mobile banking

Making financial transactions on a mobile device is mobile banking (cell phone, tablet, etc.). This activity can range from a bank sending fraud or usage activities to a client's cell phone to paying bills or moving money internationally. The ability to bank from anywhere and at any time is one of the benefits of mobile banking. Compared to banking in person or on a computer, security concerns and a limited range of capabilities are its disadvantages.

8. Bharat Interface for Money (BHIM): The National Payment Corporation of India created BHIM (NPCI). It is a mobile-based program that enables rapid, safe, and dependable cashless payments. BHMI is based on the Unified Payment Interface (UPI), allowing direct bank-to-bank e-payments. It works with other Unified Payment Interface (UPI) applications and bank accounts. The Unified Payment Interface (UPI) is an instant payment system built on top of the IMPS infrastructure that allows you to send money between any two bank accounts in real-time.

Digital Payment Prospects

Technologies that make these digital payment services possible involve machine learning and artificial intelligence. As consumers continue making purchases with their cards, mobile wallets, or applications, machine learning technology is able to study these experiences and improve them over time. This improved experience ensures greater fraud protection and security.

Additionally, contactless digital payments rely on NFC and magnetic secure transmission (MST) technology. NFC technology enables a connection between two electronic devices over a small distance. It enables consumers to pay with their mobile wallets via tablets, smartphones, or smartwatches

Open Banking APIs

Application programming interfaces (APIs) allow legacy banks to share data and information amongst one another through a third party application. APIs are used for any company (B2B, B2B2C, BaaS) to embed its products into a nonfinancial company's platform. [3]

Distributed ledger technology(blockchain)

A distributed ledger is a database that exists across several locations. Most companies use a centralized database that exists in a fixed location; but a distributed ledger removes third parties from the process.

Block chain technology offers a way to securely and efficiently create a tamper-proof log of sensitive activity. Distributed ledgers like block chain are particularly useful in the finance industry because they cut down on operational inefficiencies (saving incumbents both time and money).

CYBER THREATS IN E-BANKING

Identity Theft

Identity theft is a cyber threat in which a hacker steals someone else's financial or personal data and uses it for their selfish, illicit activities. A data breach at a bank can lead to an inflammation in identity theft cases as the stolen bank data is sold on the dark web to buyers who're willing to pay hefty amounts. The data can be used in all imaginable ways to wreak havoc.

Spoofing

This is a technological cyber threat in which a hacker mimics an official banking website and then uses spoofed email to bait victims into visiting these websites. Under some phishing pretence, the user is asked to enter their credentials in a valid-looking form, which ultimately leads to credential theft.

The username and passwords are harvested, either to be sold, or even misused by the hackers themselves to authenticate transactions and withdrawals.[3]

Ransomware

In this type of cyber-attack, the hacker injects malware into a system by means of malicious payloads delivered via phishing emails. The malware corrupts all the data on the system, can spread to other connected systems, and then lock the user out of their own system. The hacker then demands a whole lot of money in exchange for granting access back to the system.

Business Email Compromise

Like the business world, the banking sector has also adapted to email communication. Banks often send email notifications of transactions, share sensitive data with the customers over email, and use email to communicate with other branches.

At the base of a BEC attack is phishing, a method used by hackers to trick the victim into engaging with malicious links and attachments of a fraudulent email. Executed just right, phishing can lead to data theft, including a banking customer's login credentials.

Threats From an Internal Employee

Dissidence from within an organization is nothing new. Disgruntled employees, unhappy with their salaries or company policies, will often plan to revolt from the shadows. An employee with a bone to pick with a bank can cause severe damage. This may include blatantly ignoring the security practices established within a bank, or even leaking data intentionally

DDOS

Even the most robust of servers are of no use if they are tied up handling spammy requests. That is exactly what a Distributed Denial of Service attack does. Scripts are run which make unrelenting requests to a bank's infrastructure. This is more volume than the infrastructure can handle, and ultimately, it collapses

DIGITAL PAYMENT THREATS

Malware

Malicious software, or malware, refers to any software used to access third-party computers and steal or interfere with sensitive data. It comes in all forms and shapes. And with fraudsters becoming more and more tech-savvy, it's getting more difficult to identify and prevent malware attacks. Thus, among the most common types of malware are spyware, adware, Trojan horse,ransomware, fileless ware and ATPS.

Mobile Cyber attacks

With a growing dependence of a modern user on a mobile device, cybercriminals are working their way into mobile app fraud. It's less secure, and therefore, serves as an easy target for fraudsters. In fact, at least 38% of iOS and 43% of Android apps are considered "vulnerable". Moreover, with mobile devices, the fraudster no longer requires physical access to your smartphone to be able to steal sensitive data.

APT:

Some consider APT (advanced persistent threat) a type of malware. And there's a certain truth to it. APT is an attack on a specific target, be it an individual, a company, or some software. It aims to adapt to the defence techniques and change the technologies on the go.

The goals behind the attacks vary. But since most frequently APTs are targeted at government agencies and defence contractors, they're associated with cyberespionage.

Crypto jacking

With crypto currencies gaining their momentum these days, cryptojacking is coming on stage. It's mobile-related and takes place when hackers use someone else's mobile device for crypto mining without the consent of the said person.

Most victims of these threats experience very short battery life, overheating, etc, indicating extreme use of the device by the third party.

SMS Message Threats

The sad truth is SMS messages can be easily spoofed, and now more than ever with the advances of technologies available to the fraudsters. Therefore, users fall victim to smishing when they're sharing sensitive information with criminals behind SMS messages sent from a payment service provider number. They tend to create the feeling of the urgency of the measure so that the victim is less hesitant to share sensitive data with the hacker.

DIGI SECURITY TAL PAYMENT MEASURES

Email validation and authentication

Payment service providers can use these two measures to detect and prevent email phishing and spoofing early on. European Payments Council recommends using SPF and DKIM as prevention measures as well as run frequent awareness campaigns. Informed means armed, and that's exactly your users need.

Limits on the number of installed apps and cyber hygiene

Might seem obvious, but with the overwhelming volumes of software we use today, the best way to avoid malware is to limit the number of installed applications. Only download programs from trusted vendors and remember to regularly update it. Outdated apps allow fraudsters to get access to your device with you knowing it.

Monitor your mobile device closely

Not only this will allow you to notice traces f ransomware otherwise undetectable but also track any suspicious activity on the device pointing to unauthorized usage of your mobile device. And also, stay in touch with your mobile network provider. Especially so, if you notice network connectivity issues or no incoming calls for an unusually long time.

PCI DSS certification

This security standard is only one of many mandatory requirements for online merchants. It protects the user's data online. So, if you're a user, make sure to pay on sites that have this certification in place. If you're a merchant, reach out to us so we can help you obtain a certificate asap.

PAYMENT GATEWAY SECURITY MEASURES

PCI DSS Compliance

Payment Card Industry Data Security Standard, also known as PCI DSS, is a set of compliance rules and security regulations that are implemented by the major card schemes. PCI DSS compliance is a requirement for any business that processes credit or debit card transactions. Adhering to the compliance schemes ensures a secure environment for credit and debit transactions to take place, without details being vulnerable to card theft and fraud. It's important for any business that accepts online payments to understand PCI DSS standards so they can make the right choice when it comes to selecting a payments partner.

Data Encryption

Encrypting data is the main method that payment gateways use to secure sensitive transaction data. When you enter your card details at the checkout the payment gateway will encrypt the data. Encryption turns the data into another form, or code so that only people who have access to a secret key. The payment gateway will decrypt the transaction through its own private key. Doing so drastically decreases the possibility that the data can fall into the wrong hands.

Secure Socket Layer(SSL)

Secure Sockets Layer, or SSL, is a security technology that creates a safe between a payment provider and a customer's web browser. Any data that's communicated via the SSL is encrypted. All web browsers can have an SSL. If a website is processing a transaction directly, then it should have SSL in place.

Secure Electronic Transaction (SET)

Secure electronic transaction or SET is a system and electronic protocol that encrypts the payment data of credit cards. Jointly designed by the major card schemes VISA and Mastercard, SET conceals all personal details on the card, which prevents fraudsters from accessing the information

Tokenization

Tokenization is the process of converting the card holder's sensitive data into a security token. Creating a token involves hashing, encryption, and secret keys. As the card schemes prevent merchants from storing card numbers unless they are completely compliant with PCI DSS guidelines, having a payment gateway that uses tokenization is your best bet. Tokenization increases security because sensitive information is only sent once over the internet, once the token is created, it's then used for future payment requests.

3D Secure 2.0

3D Secure 2.0 (3DS 2.0, 3DS2 or EMV® 3-D Secure) is an authentication protocol developed by EMVCo to address the issue of customer authentication in online payments. When the customer has entered their card details, they will receive an extra step to verify their payment with their bank, usually via a password. It provides both the merchant and the customer an extra layer of protection against charge backs and fraud - while facilitating a frictionless and seamless payment experience across different channels.

CONCLUSION

PREVENTION IS BETTER THAN CURE...

- Prevent account data from being intercepted when entered into a mobile device.
- Prevent account data from compromise while processed or stored within the mobile device.
- Prevent account data from interception upon transmission out of the mobile device.
- Prevent unauthorized logical device access.
- Create server-side controls and report unauthorized access.

- Create the ability to remotely disable the payment application.
- Detect theft or loss.
- Harden supporting systems.
- Conform to secure coding, engineering, and testing.
- Protect against known vulnerabilities.
- Protect the mobile device from unauthorized applications.
- Protect the mobile device from malware.
- Protect the mobile device from unauthorized attachments.

Lastly – think simple steps...

- Be Vigilant
- Backup Data
- Disable Macros &
- Patch and Purge

REFERENCE:

1. Bostic, Raphael, et al. "Shifting the focus: digital payments and the path to financial inclusion." Promoting Safer Payments Innovation 20.1 (2020): 1-25.

2. VITHYA, Ms C. JAMESLYN. "Applications of digital payments in online shopping." the new era of digital Payments (2021): 78.Safa, Nader Sohrabi, Rossouw Von Solms, and

3. Steven Furnell. "Information security policy compliance model in organizations." computers & security 56 (2016): 70-82.CA, B., 2021. E-commerce.