ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XII, Issue– I (b) Jan – Feb 2023

OPEN ACCESS Original Research Article

IMPACT OF DIGITALIZATION ON RISING CASES OF CYBERCRIMES WITH SPECIFIC REFERENCE TO SALARIED PEOPLE IN MUMBAI REGION

Prof. Mansi Dangarwala,

Assistant Professor,

Ghanshyamdas Saraf College of Arts and Commerce, Mumbai.

Abstract:

Digital world has grown into many leaps and bounds as a result of multiple innovations and advances in technology. Post co-vid, there has been a humongous rise in the usage of computers and electronic gadgets. The evolution of information technology (IT) is responsible for the stupendous success of communication through internet, diverse reach of business and global interaction on social media platforms. However, it has also lead to a marginal increase in criminal activities in the cyber world.

***Cybercrimes** refers to the illegal activities that uses a computer network, or a networked device. Most cybercrimes are committed by cybercriminals or hackers to make money.*

***Cybercriminals** are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit. Cybercriminals range from individuals to criminal organizations to state-sponsored actors. Just as the type of criminal varies, so do their crimes and the methods they use to break the law. This paper describes the reasons as to why hackers commit cybercrimes, differing types of cybercrimes that are committed these days, how it is impacting the salaried people in Mumbai region and possible solutions to mitigate these attacks.*

Keywords: *Cybercrime, Digital, salaried people.*

Introduction:

New technology creates new opportunities for attackers to perform different crimes. It may be possible to determine where an attack has come from but it is impossible to determine if it has been launched by an individual or by a gang for criminal purposes. This creates difficulties in blaming and deciding what action might be appropriate.

As digitalization and the Internet of Things (IoT) evolves and smart devices become more popular, cybercriminals benefit from a much broader attack surface — increased opportunities to penetrate security measures, gain unauthorized access, and commit crimes. This has affected the salaried class functioning and the way they use digital methods in their everyday life.

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XII, Issue– I (b) Jan – Feb 2023

OPEN ACCESS Original Research Article

Reasons as to why cybercrimes are committed

- business' financial details
- customers' financial details (eg credit card data)
- sensitive personal data(eg Passwords)
- customers' or staff email addresses and login credentials
- customer databases
- clients lists
- IT infrastructure
- IT services (eg the ability to accept online payments)
- intellectual property (eg trade secrets or product designs)
- Political motivation
- Insider threats

Types of Cyber crimes

1. Phishing: When a user receives spam emails that contain unauthorized attachments or URLs luring them to open the same, it is called phishing. The objective of this act is to gain personal information of users or organizations by tricking them. Some of them may be flagged but most of them do not show the signs of any malpractice on the face. The cybercriminal may not directly harm the device being used but may cause financial loss to the user due to credentials shared, data loss due to website access that results in identity theft, etc.

Example: An email from Paytm arrives, informing the victim that their account has been deactivated and they need to confirm credit card details in order to activate it again.

2. Identity Theft: As the term itself suggests, identity theft happens when someone else impersonates the original user. The cybercriminal steals personal information of the users for fraudulent purposes. Example: Someone filing for bankruptcy under your name.

3. Social Engineering: When malicious activities are committed through the internet with a personal touch, it is termed as social engineering. They use psychological manipulation tricks through calls impersonating an official to defraud the users so that they share confidential information.

Example: Credit card fraud is usually committed in a similar way when someone calls the users, conveys to be a bank official and asks the users to share the one-time password received on their mobile to safeguard their financial interests or bank accounts.

4. Denial of Service (DoS): There are various websites that provide services online to their customers. If the website has errors in proper functioning, the services will be impacted. That is how denial of service (DoS) works. Fraudsters overwhelm the website with more traffic affecting online networks and thereby interrupting the services. Example: During the Amazon black Friday sales, legitimate users cannot access the website.

5. Ransomware: When fraudsters steal your confidential or personal information and threaten to misuse or delete the same unless the users transfer a certain amount to safeguard or access such information/ data, it is called ransomware.

Example: Ransomware attack temporarily disabled Macmillan Publishers ability to accept, process or ship orders.

6. Malware Attacks: People using smartphones with internet connection are sometimes tracked for location, for their internet searches, the usernames and password typed on their device, through web

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XII, Issue– I (b) Jan – Feb 2023

OPEN ACCESS Original Research Article

cameras, etc. At times, it could be legal and informed due to app permissions, but at other times, it may not be brought in the user's knowledge and become a serious threat to confidential data. Such an uninformed activity on devices which may sneak personal information resulting in bigger financial frauds or other threatening acts are called malware attacks.

Example: DarkHotel uses hotel Wi-Fi to gain access into the accounts of powerful people.

7. Cyberstalking: When someone follows another over social media, online websites or search engines subjecting the user to a plethora of online messages or emails threatening for his/ her safety, it is cyber stalking. In serious cases, cyber stalking may lead to 'sextortion' whereby the victim is threatened for personal pictures or videos seeking money or sexual advances from their victims. Cyberstalking could result in cyberbullying which may be a permanent threat to mental and physical health of victims.

Example: Seema Khanna (name changed), a worker at the American embassy in New Delhi, was stalked by a man who asked her to strip for him or pay him Rs.1 lakh.

Review of literature: Prevention of cybercrimes in smart cities of India: from a citizen's perspective, Sheshadri Chatterjee, Arpan Kumar Kar, Yogesh . Dwivedi, Hatice Kizgin,2019 His study reveals that the "awareness of cybercrimes" significantly influences the actual usage of technology to prevent cybercrimes in Smart Cities of India. The study reveals that government initiative (GI) and legal awareness are less influential in spreading of the awareness of cybercrimes (AOC) to the citizens of the proposed smart cities.

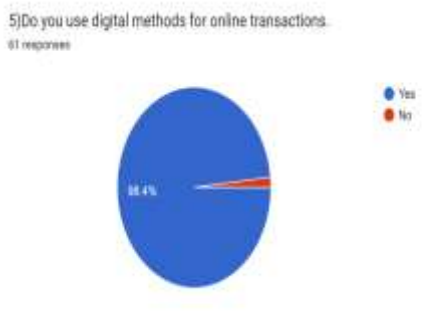
As per reports supported by the Better Business Bureau Online, over 80% of online customers referred to security as an essential concern when leading business over the Internet. About 75% of online customers end an online exchange when requested the Visa data. The observation that the Internet is overflowing with charge card extortion and security dangers is developing. This has been a major issue for web based business.

Objectives of the Study:

1. To conduct an ongoing review of the cyber security landscape and emerging threats.
2. To analyse the impact of cybercrimes on salaried employees in Mumbai region.
3. To suggest adoption of various security protocols/standard to mitigate cyber attacks.

Research Methodology: Simple Random sampling method was used to select the sample. Sample size was 61 respondents. Sampling unit used for salaried people from Mumbai region. Method of data collection was primary and secondary data. A pre-structured questionnaire was used for primary data collection and journals, research papers and books were used for secondary data collection.

Data Analysis and Interpretation:



Interpretation:

The Graph depicts that 98.4 % of respondents use

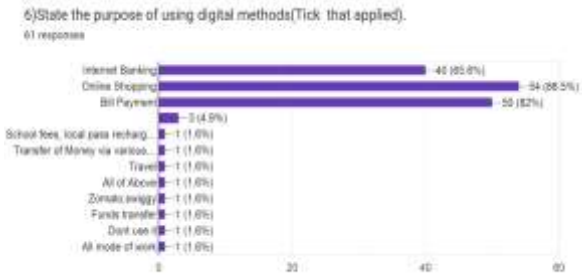
ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XII, Issue– I (b) Jan – Feb 2023

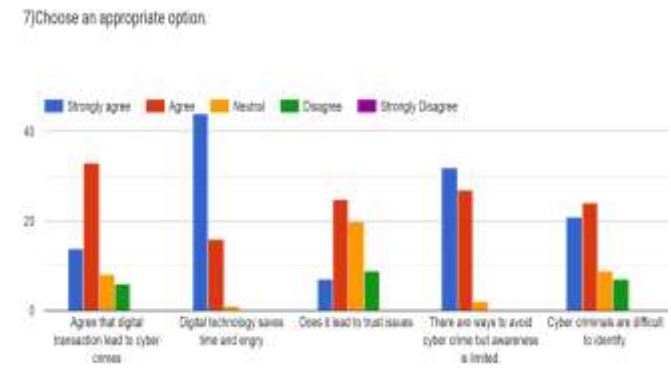
OPEN ACCESS Original Research Article

digital methods for online transactions.



Interpretation:

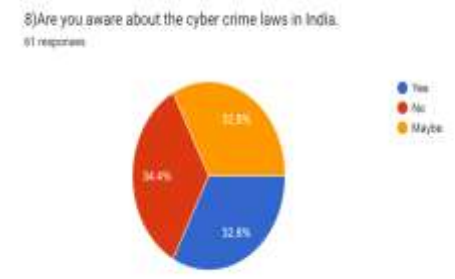
88.5 % of respondents resort to online shopping, 82 % use digital modes for bill payment and 65.6% use Internet banking in terms of digitalization.



Interpretation:

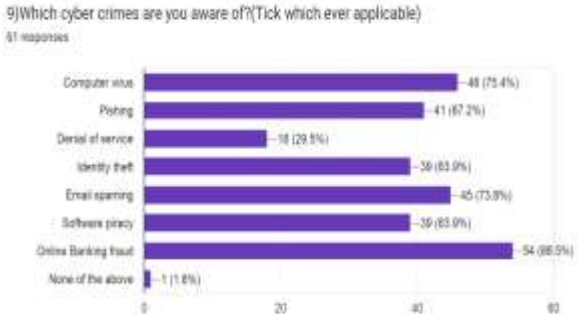
Maximum no of respondents agree that digital transaction saves time but also leads to cybercrimes, which could be avoided if there is awareness about the same.

Study also states that cyber criminals are difficult to identify and hence it leads to trust issues.



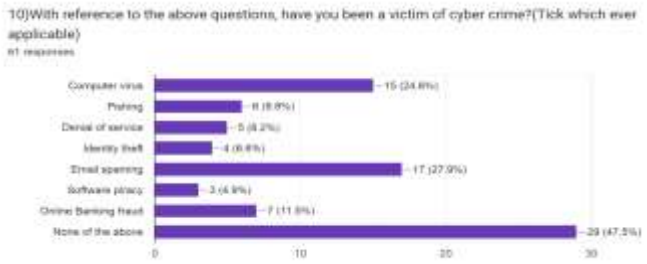
Interpretation:

More than 60% of the respondents are unaware about the cybercrime laws in India.



Interpretation:

Study shows that there is awareness amongst respondents about various cybercrimes with online banking being the highest with 88.5 %. Computer virus (75.4%) and Email spamming (73.8%) being the next most known cybercrime followed by phishing (67.2%) and Software piracy (63.9%). Denial of service is the least known cybercrime with 29.5 % respondents being aware about it.



Interpretation

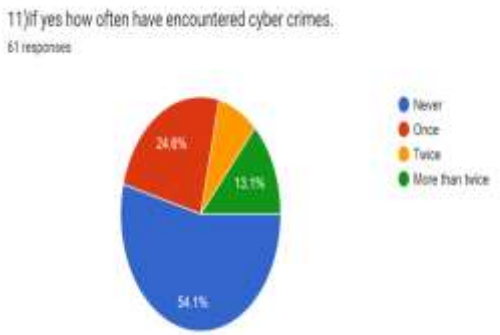
Almost half of the respondents have not been a victim of cybercrime. Study shows that Email spamming with 27.9 % is the most frequent cybercrime that respondents have been victim of followed by computer virus with 24.6 %.Third most encountered cybercrime was online banking with 11.5%. Very few respondents were a victim of Phishing, denial of service and software piracy.

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

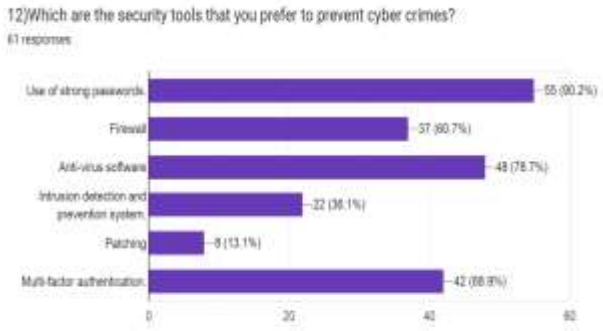
Volume–XII, Issue– I (b) Jan – Feb 2023

OPEN ACCESS Original Research Article



Interpretation:

Study shows that half of the respondents have never encountered cybercrime. 24.6 % of respondents have experienced them once followed by 13% to have experienced it more than twice. 8.2 % of respondents have been a victim of cybercrime twice.



Interpretation:

Study shows that usage of strong passwords with 90.2% respondents find it as an effective tool against cybercrime prevention followed by installation of antivirus software with 78.7%. Multifactor authentication mechanism, with 68.9% respondents feel the need to use in order to mitigate cybercrimes. Incorporation of firewalls to protect the network form being attacked by cybercriminals has been agreed by 60.7% respondents. 36.1 % respondents suggest that implementation of intrusion detection and prevention systems for continuous monitoring of networks will lead to decrease in cybercrimes followed by patching with 13.1 % for system to be continuously updated.

Findings:

1. Study shows that digital methods are extensively used for online transactions.
2. It has been observed that the most popular digital methods used by maximum respondents are online shopping, bill payments and internet banking.
3. Most of the respondents agree that digital technology saves time but also leads to cybercrimes.
4. The research also indicates that majority of the respondents are aware about various types of cybercrimes and some of them have been a victim of it.
5. Use of strong passwords and antivirus software are the most preferred tools by respondents to combat cybercrimes.

Limitation of Study:

1. The study was conducted on a low sample unit of Mumbai region.
2. Due to time constraints, the sample size was limited to 60 respondents.
3. Biasness of the respondents may affect the result of the study.

Suggestions:

1.Protect systems/devices through security software such as anti-virus with the latest version.

2. Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.

3. Ensure all devices/accounts are protected by a strong PIN or passcode. Never share your PIN or

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XII, Issue– I (b) Jan – Feb 2023

OPEN ACCESS Original Research Article

password with anyone.

4. Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.
5. Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.
6. Do scan all e-mail attachments for viruses before opening them. Avoid downloading e-mail attachments received in e-mails from unknown or un-trusted sources.
7. Be careful while sharing identity proof documents especially if you cannot verify the authenticity of the company/person with whom you are sharing information.

Conclusion:

As per the World Economic Forum's Global Risks Report 2021, cyber risks continue to rank among global risks. Being a cybercriminal offers big rewards and few risks since, until recently, the likelihood of detection and prosecution of a cybercriminal was estimated to be very low. Policymakers can help by working with cybercrime experts to establish internationally accepted criteria for attribution, evidence, and cooperation in pursuing cyber criminals and bringing them to justice. Salaried individuals, especially with high assets need to incorporate cyber security features while using the internet. If any misuse of your data is seen, then visit the website of National Cyber Crime Reporting Portal at https://cybercrime.gov.in/ The complainant shall choose the option of "Report and Track" while initiating the registration of complaint on the portal and register himself/herself with the use of his/her name and valid Indian mobile number.

References:

Bibliography:

1) Rhodes-oulsey,Mark, "The complete Reference: Information Security".
2) Arthur Conklin and Greg White "Principles of Computer Security"

Webliography

https://cybercrime.gov.in/pdf/Cyber%20Security%20Awareness%20Booklet%20for%20Citizens.pdf

https://ieeexplore.ieee.org/abstract/document/9167567/figures#figures

https://scholar.google.com/scholar?as_q=Security+Analytics%3A+Big+Data+Analytics+for+Cybersecurity&as_occt=title&hl=en&as_sdt=0%2C31

Cite This Article:

Prof. Dangarwala M., (2023). *Impact of Digitalization on Rising Cases of Cybercrimes With Specific Reference to Salaried People in Mumbai Region,* ***Electronic International Interdisciplinary Research Journal****, XII, Issue – I(b), Jan-Feb, 94-99*

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XII, Issue– I (b) Jan – Feb 2023

OPEN ACCESS Original Research Article