Citation: Shahzad, M. (2023). Emerging Cyber Crimes in Pakistan: A Case Study of Online Fraud through Digital Microloan Apps. *Global Digital & Print Media Review*, *VI*(II), 411-421. https://doi.org/10.31703/gdpmr.2023(VI-II).30

- **Vol.** VI, **No.** II (Spring 2023)
- **Pages:** 411 – 421
- **p- ISSN:** 2788-4988
- **e-ISSN:** 2788-4945

- **URL:** http://dx.doi.org/10.31703/gdpmr.2023(VI-II).30
- **DOI:** 10.31703/gdpmr.2023(VI-II).30

Muhammad Shahzad *

Emerging Cyber Crimes in Pakistan: A Case Study of Online Fraud through Digital Microloan Apps

Abstract: *This study aims to investigate the newly emerging phenomenon of cyber-crimes in Pakistan with the lens of a case study focusing on online fraud through digital microloan apps. The study employed qualitative methodology with an inductive approach of thematic analysis to examine the responses of interviewees. This thematic approach allowed the emergence of themes from the data. A sample size of 15 male and female students was chosen from 5 Public and private sector Universities of Lahore. The study found that online fraud through microloan apps has become a common phenomenon in Pakistan with weak implementation of cyber-laws, thus putting most social media users especially those who are using online digital apps to acquire microloans under the threat of cyber-fraud. The study also found that female students were comparatively easy prey to these loan apps than male students. The study recommended that public and private media houses launch an awareness campaign among digital media users to avoid such kind of fraud. The study further recommended that law enforcement agencies should ensure strict implementation of cyber-security laws to ensure a safe and secure environment.*

Key Words: Cyber-Crimes, Cyber Security, Microloan, Social Media, Thematic Analysis

Corresponding Author: Muhammad Shahzad (Assistant Controller, Examination Branch, University of the Punjab, Lahore, Punjab, Pakistan. Email: imranshah2036@gmail.com)

Introduction

Criminal activity emerged on this planet with the arrival of a human being on this earth. Crimes took various shapes in various parts of the world (Wyatt, 2021). However, the emergence of technology reshaped criminal activities in the modern era. The population of the entire world is surpassing 7.5 billion people now. The rapid growth of technology and the internet has brought unprecedented opportunities for communication, e-commerce, e-learning, public health, social relations and e-coherence across the world in general and in Pakistan in particular (Cleghorn, et al., 2019; Heeks, et al., 2001; Slim & Hafedh, 2019). However, alongside these benefits, there has been a surge in cybercrime, presenting new challenges to individuals, business organizations, and state-level cyber-security. Cybercrime is an emerging phenomenon in Pakistan because of multiple factors (Jamshed, Rafique, Baig, Ahmad, & Affairs, 2022). In such a case scenario, electronic devices, mostly smartphones;

* Assistant Controller, Examination Branch, University of the Punjab, Lahore, Punjab, Pakistan.

laptops/ desktop computers, SIM Cards and other electronic gadgets are utilized through the internet to commit digital crimes (Glisson, Storer, Mayall, Moug, & Grispos, 2011). Basically, cybercrimes are jeopardizing the social, economic and political well-being of the individual as well as leaving severe impacts on the individual's life safety (Bada & Nurse, 2020). Half of the World population is excessively using social media platforms through smartphones or other gadgets, which consequently increases cybercrimes. Cyber-crimes have been divided into different types including hacking, money laundering, cyber-bullying, data theft, Malware, financial theft, and electronic terrorism etc. (Memon, Mahar, Dhomeja, & Pirzado, 2015). People of different age groups are involved in cyber-crimes ranging from 18 years to onward. For instance, the cybercrime cell of the Federal Investigation Agency of Pakistan (FIA) has traced people in different age groups and from different professions. The data of the FIA revealed that the persons involved in grocery, vegetables, businessmen, sales persons and other businessmen are involved in cyber-crimes (Shahid, Kauser, Zulqarnain, & Pakistan, 2018).

There is a long list of cybercrimes ranging from child pornography, theft of intellectual property, fraud, exploitation, and individual and country security issues. Phishing attacks involve fraudulent attempts to obtain sensitive information of individuals, banks or security-related departments, such as passwords, credit card details, and personal identification (Ekawade, Mule, & Patkar, 2016). According to the common practice that started in near about 2005, the criminals involved in cyber-criminal activities were using ransomware; a kind of malware by sending deceptive emails or messages to trick individuals into revealing their private data. Identity theft often follows, with criminals using the stolen information for financial gain or other malicious activities. This malware encrypts the victim's data, rendering it inaccessible until a ransom is paid to the attacker. Pakistan has witnessed a rise in ransomware attacks targeting businesses, hospitals, and even government institutions, causing significant financial losses and disruptions to critical services. The antivirus companies and security-related media developed anti-viruses to encounter this digital criminal activity (Kausar, Leghari, & Iftikhar, 2023; Gazet, 2010; O'Kane, Sezer, & Carlin, 2018).

The digital age has seen an increase in online harassment and cyber-bullying, where most of the time youth as well as adults are involved with offensive content, threats, or false information. However, scholars have not devised any permanent definition of Cyberbullying yet (Wolak, Mitchell, & Finkelhor, 2007; Sezer & Tuncer, 2021). Furthermore, social media platforms and messaging apps have become hotspots for such activities, affecting mental health and well-being. With the rapid growth of e-commerce and online banking across the globe, financial fraud has become a grave concern. Cybercriminals engage in activities like credit card fraud, online scams, and unauthorized fund transfers, exploiting vulnerabilities in online payment systems. Data breaches involve unauthorized access to sensitive data, such as personal information, financial records, and trade secrets (Ahmad, Iqbal, Jamil, & Kamran, 2021; Sabillon, Cavaller, Cano, & Serra-Ruiz, 2016). These breaches not only compromise individuals' privacy but also have serious implications for businesses and institutions that fail to protect their customers' data. Pakistan has witnessed instances of cyber espionage, where foreign entities attempt to gain unauthorized access to sensitive government or corporate information. This can have national security and economic repercussions (Ali, Shah, Qureshi, & Tanveer, 2022). The intelligence agencies of Pakistan have identified various *"modus operandi"* (mode of operation) of cyber-criminals who have been found involved in breaking the cyber security systems of Pakistan to gain access to the personal data of individuals. The Pakistani agencies, however, are in a race to safeguard citizens' data, personal secrecy, and personal information from unauthorized access by the intelligence agencies. Social engineering involves

manipulating individuals into divulging confidential information through psychological manipulation. This can include tactics like pretexting, baiting, and tailgating, and it's often used as a precursor to other cyber-crimes (Lomas & History, 2021; Rauf, Khan, Awan, Shahzad, & Husaan, 2022).

Impact on Society and Economy

The emerging cyber crimes in Pakistan have far-reaching consequences. The rise of online digital microloan app fraud has profound impacts on individuals and society. Individuals and businesses face substantial financial losses due to fraud, ransom payments, and legal expenses arising from cyber-attacks. Victims of this fraud may face significant financial losses, as their personal information is misused to obtain loans they never applied for. In the last two decades, Pakistan has witnessed a multiplier effect in cybercrimes due to a lack of digital forensic scientists and crime-investigating specialists. Even no legislation had been made on cybercrime until the Prevention of Electronic Crimes Act (PECA) 2016 (Kumar & Sciences, 2023; Rauf, et al., 2022). The breach of personal and sensitive data erodes citizens' privacy, leading to identity theft and unauthorized use of personal information. Personal and financial information of individuals is compromised, leading to potential identity theft and further financial risks. Unpaid loans obtained through fraud can damage the victims' credit scores, affecting their ability to secure legitimate loans in the future. Cyber-attacks can tarnish the reputation of businesses, government bodies, and individuals, affecting their credibility and trustworthiness. The emergence of online microloan apps' fraud erodes trust in digital financial services, hindering the adoption of legitimate platforms. Ransomware attacks and other forms of cyber-attacks can disrupt critical services, affecting healthcare, transportation, and public utilities. Online harassment and cyberbullying can lead to psychological distress, anxiety, and depression among victims (O'Kane, et al., 2018; Victoire et al., 2023).

The National Security Advisor (NSA), a senior official of the National Security Council of Pakistan has released a report in the recent past, which has underlined security flaws in Pakistan. The report revealed that the personal data of individuals can be used for unlawful purposes due to flaws in the cyber security systems in Pakistan (Jamil & Studies, 2021). The report suggested that the Pakistani government must step forward to ensure the safety of the personal data of the individuals thus combating the cyber security threats. According to a study, a total of 624 customers from twenty-two banks in Pakistan suffered a monetary loss of $11.7 million in the wake of a cyber-attack in November 2018. Moreover, the FIA revealed that hackers sold the data of 19,865 ATM cards to the dark web in Pakistan in the same year. The Cyber-Crime cell of the FIA also claimed to have arrested 16 persons involved in cyber-attacks in Pakistan. In the wake of the looming threats of cyber-attacks, job opportunities have increased multifold in Pakistan to safeguard against cyber-attacks and cyber-crimes (Anjum, 2020).

Literature Review

The technological advancement and widespread internet connectivity in Pakistan have paved the way for innovative financial solutions, including digital microloan apps that offer quick and convenient access to loans. However, this convenience has also given rise to emerging cyber crimes, particularly online microloan app fraud. This case study delves into the details of this specific cybercrime, analyzing its methods, impacts, and potential preventive measures. Online microloan apps have gained popularity in Pakistan as they provide an alternative to traditional bank loans. A study revealed that these apps offer a simplified application process, quick approval, and disbursal of funds directly to users' bank accounts or smartphone cash apps (Rizvi, Naqvi, & Tanveer, 2018).

Pyke et al., (2021) conducted a study to examine factors that obstacle users from identifying the intensity of cyber-attack. They examined the knowledge of individuals who were facing cyber-attacks, their inclination

towards the use of technology, their emotions, arousal and abrupt response to cyber-attacks. The study found that the persons affected by low-risk attacks were less provoked whereas, high-risk attacks provoked more arousal and negative emotions among the victims. The study further found that the persons having high knowledge successfully identified the attacks as compared to the peers with low knowledge. Thus, the study suggested that the users with high knowledge have a greater propensity to trust the technology. Similarly, the study further suggested that when users face cyber-attacks, their situational trust is low whereas, the emotional response is high to handle the risk.

A study examined that there were quite negative market returns due to security breaches and rapid announcements of cyber-attacks in addition to the negative effects on financial institutions. The non-confidential cyber-attacks are dangerous for the stability of financial institutions as compared to other consistent attacks. Unfortunately, this convenience has attracted the attention of cyber criminals who exploit the vulnerabilities in these platforms for financial gain (Smith, et al., 2019).

According to another study, cybercriminals create fraudulent apps that closely resemble legitimate online microloan apps. Unsuspecting users download these apps, believing them to be authentic, and unwittingly provide sensitive personal information. Criminals use phishing techniques to trick users into revealing their personal and financial information through fake messages, emails, or websites that appear to be from legitimate credit app providers (Alkhalil, Hewage, Nawaf, & Khan, 2021). The findings of the study revealed that cyber criminals may use stolen identities to apply for loans on these platforms, leaving the victim to deal with the consequences of unauthorized debt. A study shared that fraudsters apply for multiple loans from different online microloan apps simultaneously, often using false information, with no intention of repaying the loans. Criminals take advantage of lax identity verification processes to swap the victim's SIM card, gaining access to their mobile number and subsequently to their credit app accounts (Gies, Piquero, Piquero, Green, & Bobnis, 2021).

A study suggested that the internet has made it possible for all to develop network connectivity thus leading towards information progression in cell phones, laptops, computers and other online games or other digital platforms. A study revealed that internet services were available across the country with the establishment of the Pakistan Telecom Company Ltd. (PTCL) which provided internet connectivity to all the consumers in the 19th century. The advent of the internet reduced paperwork and shifted all the paperwork to digital working on desktop computers, laptops and cell phones (Haleem, Javaid, Qadri, Suman, & Computers, 2022).

Another study showed that the cyber-criminals were breaching security with rapid cyber-attacks in Pakistan. For instance, the cyber-criminals initially gain access to the core of the network of national and multi-national organizations. In 2017 alone, a study shared that a 67 per cent rise in cyber security violations was witnessed during the last five years (Maluleke & Review, 2023). The findings of the study revealed that cyber-attackers were used to employ modern techniques for carrying out cyber-attacks; they breach the security of business plans of national and international organizations to gather information online. The findings revealed that cyber-criminals were financially advanced; therefore, they enable themselves to involve internet users in their cyber-attacks in stealing their privacy besides stealing their credit cards and other details (Ibarra, Jahankhani, Kendzierskyj, & Data, 2019).

According to He & Security (2013), 45 per cent of mobile users have smartphones having more storage capacity as compared to the past; therefore, they have given access to hackers to their personal information. Most of the people in the old or average age group are technologically less advanced therefore a hacker can easily hack their individual data by gaining access to their smartphones and other devices i.e., laptops, tablets or desktop

computers linked to the internet. A study revealed that cyber-criminals can easily access discussions, business negotiations other business strategies and other confidential information even the smartphone users have installed anti-virus in their phones to protect them (He & Security, 2013). The findings of the study say that mobile phone breaches are a common phenomenon among cyber-criminals; therefore, apps being used on smartphones can easily be hacked by criminals. According to a study, cyber-criminals have developed malware programs to get easy access to Wi-Fi passwords, to steal passwords of credit cards, mobile phone apps and other online platform business tools by taking advantage of the existing security flaws (Igor et al., 2013).

According to Ashraf, König, Javed, & Mustafa (2023) people can lodge a complaint with the FIA through the online emailing system by calling at helpline number 9911 or physically visiting the FIA cyber-crime cell. However, most of the people avoid visiting the FIA because they are unsure about the ultimate end of the complaint. According to a study, almost 95 per cent of people avoid lodging a complaint with the FIA because they believe by registering the complaint they would become more vulnerable to the hands of the hackers especially when the photos and personal data of the females are uploaded on Facebook, Instagram and other social media platform.

Knowledge Gap

After a detailed literature review, the study found that there was a huge gap in carrying out academic studies on online digital microloan apps in Pakistan. The literature search revealed that extensive studies have been conducted with different lenses but the least attention has been given towards carrying out any research-oriented study on financial institutions or credit and other online apps. The literature showed that cyber-security was under acute pressure in Pakistan because the people with less awareness about online fraud and fraudulent practices by the cyber-attacks were posing severe threats to individual security.

Problem Statement

Each technology has some advantages and some disadvantages. The Internet was once considered to be one of the greatest blessings on the planet. The Internet played a vital role in expanding technological advancements like desktop computers, laptops, tabloids, mobile phones and other tech gadgets. However, technological advancement brought certain disadvantages as well. For instance, the phenomenon of cybercrime created a gigantic problem for all sorts of businesses i.e., baking, the IT sector, corporate sector, private and public institutions. Cybercrime has emerged as a new phenomenon, which created massive problems for each sector. The national as well as international organizations are facing this problem to a great extent. Hacking baking accounts, personal data, mobile phones and laptops are a few examples which have infringed the fundamental rights of privacy of almost every individual using any tech-related gadget.

Significance of the Study

This study is significant in the sense that it covers the unique phenomenon of emerging cyber-crimes in Pakistan. This study may open new horizons for the researchers pertaining to finding ways to tackle this emerging phenomenon of cyber-crimes in Pakistan. This study is an effort to identify the problems generated by the cyber-crimes and find out doable solutions to those tech-related problems. The researcher has made an effort to find the gaps and problems, which the people especially the individuals are confronting in public as well as private sector organizations.

Research Objectives

The following objectives have been chosen to achieve through this study: -

1) To analyze fraudulent practices regarding online microloan apps in Pakistan.

2) To examine the existing situation of cyber-crimes with online microloan apps in the country.

Research Questions

1) What are the fraudulent practices regarding online microloan apps' in Pakistan?
2) What is the existing situation of cyber-crimes with online microloan apps in the country?

Research Methodology

This study employs qualitative methodology to explore the phenomenon of cyber-crimes regarding online microloan apps' in Pakistan. The study employed qualitative methodology with an inductive approach of thematic analysis to examine the responses of interviewees. This thematic approach allowed the emergence of themes from the data. Although it's a general phenomenon and a common issue being confronted by online microloan app users for multiple reasons, the victims of cyber-crimes avoid reporting such crimes to the FIA or any other lawful authority, otherwise, the quantitative approach could have been the most appropriate methodology for this study to discuss this general phenomenon. This study has further employed thematic analysis techniques to analyze the data.

Universe of the Study

All the young population i.e., youth has been taken as a universe of the study, because the entire population cannot be taken to examine their problems and summarize the results within a limited timeframe.

Population of the Study

This study has considered the youth between the age group of 18-25 years of Lahore as the population of the study. Lahore is believed to be the diverse city of Pakistan which hosts the population with all demographics from all over the country.

Sample Size

The researcher has identified and chosen 15 respondents from five universities including three public and 2 private sector universities of Lahore. These respondents were the direct victims of the online microloan apps' fraud at various times; therefore, these seemed the most appropriate respondents for the study in hand.

Data Analysis

The study employed a coding sheet which carried themes, categories and codes extracted from the collected data from the respondents. The data has been analyzed using the thematic analysis technique manually. The following three themes were developed from the qualitative data.

a. Fraudulent Practices in Online Digital Microloan Apps
b. Cyber-crimes pose threats to individual security
c. Preventive Measures to Counter Cyber-Crime

Theme No. 1

Fraudulent Practices in Online Digital Microloan Apps

According to a respondent who was a first student of MBA at the University of the Central Punjab, Lahore; he shared as,

"I was the first victim of cybercrime in my class when I first learnt that the amount of my University's fee was stolen from my bank account and that was shocking for me. The bank manager expressed his helplessness on the incident rather he shared with me it was the 7th incident of cyber-crime in the same bank".

Accordingly, another respondent from the University of Punjab, who conditioned anonymity due to multiple reasons, revealed that he confronted a cyber-crime act in the recent past. The respondent said,

"My Facebook account was hacked by criminals for merely thirty minutes. It seemed a casual thing because I could not notice for one and half hours but when I checked my Bank's Online App, then, I

learnt that I was looted as Rs.150, 000/- were withdrawn from the mobile app".

A female student of the University of Management Technology Lahore, who also conditioned anonymity, revealed that her colleague was deprived of the amount she tried to invest online and within a couple of days; she lost her trust in mobile apps. The respondent revealed as,

"Maira Latif is my fast friend. She learnt from her friends that some sort of online company had introduced an online game, where any individual could invest a certain amount and could get manifold benefits within days. Initially, she withdrew a couple of thousand but when she invested a heavy amount online, but altogether she learnt the link was down to the said website and later she reported to FIA that her money was drowned".

Interpretation of Theme: - this theme says that the people involved in cyber-crime activities have introduced several modus operandi to loot money by fraudulent practices. Different companies and criminals have chalked out several ways to loot money through online platforms. For instance, websites, online microloan apps, bank accounts, email addresses, Facebook and other social media platforms were being used by the criminals to loot innocent people.

Explanation of Theme: - According to this theme, the criminals have adopted modern means for carrying out their fraudulent practices to mint money. Online microloan apps are used by criminals to hack passwords in the name of various online games. For instance, the criminals involved in cyber-crimes have developed online games, which engage innocent users by asking them to provide passwords and details of their credit cards and other online accounts.

Theme No. 2

Cyber-crimes pose threats to individual security

Cybercrime has become a potential threat to the safety and security of individuals in any country across the globe. A respondent Faiza Malik, a student from the Department of Chemistry, University of the Punjab stated,

"With the advent of the internet, cyber crimes have become a story of the town. In fact, we are the self-victims of our own social media activities on various social media platforms. Social media platforms like Facebook, Instagram, LinkedIn, Twitter, Snapchat, and other social media handlers are the sweet-dish platforms for the hackers".

Accordingly, another respondent Arham Channar revealed his own story that how his social media account i.e., Facebook was hacked by a local hacker for three days and several of his friends were asked to send money to his (hacker) account. According to him,

"My Facebook account was hacked and the hacker started requesting money from several of his friends. Later on, I learnt from my friends who contacted me on WhatsApp via cell phone that someone impersonating him was asking for money".

Similarly, another respondent Rimsha Khan (codename), a student of the Media and Mass Communication Department at, the University of the Central Punjab, revealed that someone hacked his cell number and made a WhatsApp account with her picture as DP.

"I was surprised rather shocked to know when some of my friends sent me screenshots wherein the hacker was using indecent and objectionable language. My personal privacy was strongly damaged at the hands of hackers involved in cyber-crime. I lodged a formal complaint with the Cyber-Crime Cell of the FIA Lahore and they continued searching for the hacker but no result was found till the last hearing".

Interpretation of Theme: - the most appropriate quotes of the selective respondents were selected for this theme. This theme reveals that the hackers are targeting the personal privacy of the individuals. Cybercrime has become a potential threat for social media users and all the social media platforms were the soft target of the hackers.

Explanation of Theme: - The above-said theme reveals that cyber-security discipline should be empowered and mandatory courses should be included in the curriculum of all the subjects including engineering, agriculture

and other subjects. Social media is being used almost by every individual with a smartphone, therefore, social media literacy, education and training about cyber security laws have become vital components of our formal and informal education. Law enforcement agencies should be synchronized with the media regulatory authorities so that every possible victim of cybercrime on social media platforms should be provided justice.

Theme No. 3

Preventive Measures to Counter Cyber-Crime

In the wake of the above-said themes, it has also become imperative to devise a counter strategy to curb cyber crimes. According to a respondent, seeking anonymity,

"*Although different government agencies have devised laws to curb cyber-crimes nothing has been changed yet on the national phenomenon. Every 2nd or the 3rd person is a victim of cyber-crime but none of the government organizations have taken any remedial measure to provide justice to the victims of cyber-security*".

Likewise, a female respondent from the University of Lahore revealed that she was studying Political Sciences, when she became a victim of the cyber-crime. She reported the case with the FIA but every time, the law enforcement agency personnel used to call her but after the third to fourth hearing, she shunned visiting the office because the hacker could not be traced. In fact, his links were found out of the country. So, finally, I left pursuing the case. Accordingly, another respondent Fayyaz Ahmad Jhandeer, a student of Cyber-Security, revealed that he was in a good position to explain this phenomenon because he has gone through multiple courses in cyber-security. According to him,

"*Comparatively, cyber-security was the new discipline for the students here in Pakistan. The Western world has moved to the advanced level of cyber-security and Pakistani students were far behind in this regard. Even then, we are learning a lot of things which can be helpful in curbing cyber-security issues here in Pakistan*".

Interpretation of Theme

The responses of various respondents depict that cyber-security was a comparatively new subject for students in Pakistan. Cyber-security is a new phenomenon for most of the victims of cyber-crimes and the world has moved to the next stage to curb such sorts of crimes. There is a lack of inclusion of courses about learning, education and training regarding cyber-crime laws in different disciplines. Therefore, social media and cyber-security literacy is quite weak in Pakistan.

Explanation of Theme

This theme itself explains the deteriorating situation of cybercrime laws in Pakistan. Almost every individual has become a victim of cyber-security and every social media user was vulnerable to cyber-crimes. The female victims of the cyber-crimes avoid visiting law enforcement agencies and they feel insecure in this regard.

Findings and Discussion

The study found that social media platforms are the soft targets of the criminals involved in cyber-crimes. Social media platforms are the most appropriate platforms for easy targets because hackers are keeping an eye on such platforms, wherein social media users themselves provide their basic information, which is misused by criminals. The study further found out that most of the female students become easy targets of cyber-crimes because lack of information about cyber-security and other safety measures. Most of the online microloan apps are being used without having appropriate education and proper training of the users. Mostly, users of social media and online microloan apps are ignorant of the operational strategies; therefore, proper educational and training programs should be devised. Most of the youngsters lack proper education about cyber-security and cyber-crimes laws; therefore, they are afraid of visiting law enforcement agencies, especially the FIA. The study found out that proper courses should be included in all disciplines for proper education and training of the individuals for a safe and secure environment

and complete safety of the online microloan app users.

Conclusion

The study concludes that the emergence of cyber-crimes in Pakistan poses significant challenges to individuals, businesses, and the government. By implementing comprehensive strategies that include legal reforms, public awareness campaigns, enhanced cyber security measures, and international cooperation, Pakistan can effectively address these challenges and create a safer digital environment for its citizens. It's crucial for all stakeholders to collaborate in order to mitigate the impact of emerging cyber crimes and safeguard the nation's digital future. The emergence of online microloan apps fraud in Pakistan highlights the need for proactive measures to secure digital financial services. By implementing stricter regulations, enhancing user education, and fortifying the security measures of these platforms, Pakistan can combat this emerging cybercrime and create a safer online financial environment for its citizens. It is crucial for the government, regulatory bodies, financial institutions, and users to collaborate in order to effectively mitigate the risks posed by online microloan apps' fraud.

Suggestions and Recommendations

The researchers have made the following suggestions and recommendations keeping in view the study in hand: -

1. Strengthening cybercrime legislation and providing law enforcement agencies with the necessary tools and training to investigate and prosecute cyber criminals is essential.
2. Educating individuals about safe online practices, recognizing phishing attempts, and reporting suspicious activities can help prevent cyber crimes.
3. Businesses and organizations should invest in robust cyber security measures, including firewalls, encryption, and regular security audits to protect sensitive data.
4. Collaboration between the government, private sector, and international organizations can facilitate information sharing, threat intelligence, and joint efforts to combat cyber crimes.
5. Developing local expertise in cyber-security through training programs and educational initiatives can enhance the country's ability to prevent and respond to cyber threats.
6. Embracing advanced technologies such as artificial intelligence and machine learning for threat detection and prevention can bolster cyber-security efforts.
7. Regulatory authorities should implement stringent rules for online credit app providers, including thorough identity verification processes and data protection standards.
8. App stores should enhance their review processes to detect and remove fraudulent apps before they can reach users.
9. Individuals should be educated about the risks of online microloan apps' fraud, the importance of verifying app legitimacy, and the need to protect their personal information.
10. Online microloan apps should implement robust two-factor authentication methods to ensure that only authorized users can access and use the platforms.
11. Continuous monitoring of app activities can help identify suspicious patterns and detect fraudulent activities early.

References

Ali, S., Shah, S. Z. H., Qureshi, S. N., & Tanveer, S. (2022). Impact of Cyber-Terrorism on National Security of Pakistan. *PalArch's Journal of Archaeology of Egypt/Egyptology, 19*(3), 1456-1468. https://ssrn.com/abstract=4255891

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*(1). frontiersin. https://doi.org/10.3389/fcomp.2021.563060

Anjum, U. (2020). *Cybercrime in Pakistan; detection and punishment mechanism*. https://thesis.pide.org.pk/thesis/cyber-crime-in-pakistan-detection-and-punishment-mechanism/

Ashraf, A., König, C. J., Javed, M., & Mustafa, M. (2023). *"Stalking is immoral but not illegal": Understanding Security, Cyber Crimes and Threats in Pakistan*. Paper presented at the Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023).

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92): Elsevier.

Cleghorn, C., Wilson, N., Nair, N., Kvizhinadze, G., Nghiem, N., McLeod, M., & Blakely, T. (2019). Health Benefits and Cost-Effectiveness From Promoting Smartphone Apps for Weight Loss: Multistate Life Table Modeling. *JMIR MHealth and UHealth*, *7*(1), e11118. https://doi.org/10.2196/11118

Ekawade, S., Mule, S., & Patkar, U. (2016). Phishing attacks and their prevention. *2*(12).

Ernawati, K., Nugroho, B. S., Suryana, C., Riyanto, A., & Fatmawati, E. (2022). advantages of digital applications in public health services on automation era. *International Journal of Health Sciences*, *6*(1), 174–186. https://doi.org/10.53730/ijhs.v6n1.3684

Gies, S. V., Piquero, N. L., Piquero, A. R., Green, B., & Bobnis, A. J. C. j. p. r. (2021). Wild, wild theft: Identity crimes in the digital frontier. *32*(6), 592-617. https://doi.org/10.1177/0887403420949650

Glisson, W. B., Storer, T., Mayall, G., Moug, I., & Grispos, G. (2011). Electronic retention: what does your mobile phone reveal about you? *International Journal of Information Security*, *10*(6), 337–349. https://doi.org/10.1007/s10207-011-0144-3

Heeks, R. (2001). Understanding e-Governance for Development. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3540058

Haleem, A., Javaid, M., Qadri, M. A., & Suman, R. (2022). Understanding the role of digital technologies in education: A review. *Sustainable Operations and Computers*, *3*(3), 275–285. https://doi.org/10.1016/j.susoc.2022.05.004

Ibarra, J., Jahankhani, H., & Kendzierskyj, S. (2019). Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime. *Blockchain and Clinical Trial*, 115–137. https://doi.org/10.1007/978-3-030-11289-9_5

Igor, Z., Dmitry, M., Andrey, S., Dmitry, K., Anastasia, T., & Alexander, Z. (2013). Security Software Green Head for Mobile Devices Providing Comprehensive Protection from Malware and Illegal Activities of Cyber Criminals. *International Journal of Computer Network and Information Security*, *5*(5), 1–8. https://doi.org/10.5815/ijcnis.2013.05.01

Jamshed, J., Rafique, W., Baig, K., Ahmad, W., & Affairs, E. (2022). Critical Analysis of Cybercrimes in Pakistan: Legislative Measures and Reforms. *7*(1), 10-22. https://doi.org/10.24088/ijbea-2022-71002

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81–

97. https://doi.org/10.1016/j.cose.2017.04.005

Maluleke, W. (2023). Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa. *International Journal of Social Science Research and Review*, *6*(6), 223–243. https://doi.org/10.47814/ijssrr.v6i6.1360

Memon, S., Mahar, S., Das Dhomeja, L., & Pirzado, F. (2015, June 1). *Prospects and challenges for social media in Pakistan*. IEEE Xplore. https://doi.org/10.1109/CyberSA.2015.7166124

Pyke, A., Rovira, E., Murray, S., Pritts, J., Carp, C. L., & Thomson, R. (2021). Predicting individual differences to cyber attacks: Knowledge, arousal, emotional and trust responses. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *15*(4). https://doi.org/10.5817/cp2021-4-9

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks and cybercrime. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. https://doi.org/10.1109/icccf.2016.7740434

Shahid, K., Kauser, S., & Zulqarnain, W. (2018). Unveiling The Evil; Pakistani Young Girls And Online Harassment. *Cybercrime Journal of Research and Reviews in Social Sciences Pakistan*, *1*(2), 152–163. https://journal.kinnaird.edu.pk/wp-content/uploads/2018/12/5UNVEILING-THE-EVIL-PAKISTANI-YOUNG-GIRLS-AND-ONLINE-HARASSMENT-1.pdf

Slim, H., & Hafedh, M. J. T. e. w. t. (2019). Social media impact on language learning for specific purposes: A study in English for business administration. *Teaching English with Technology 19*(1), 56-71. https://tewtjournal.org/download/5-social-media-impact-on-language-learning-for-specific-purposes-a-study-in-english-for-business-administration-by-hadoussa-slim-and-menif-hafedh/

Smith, K.T., Jones, A., Johnson, L. and Smith, L.M. (2019), "Examination of cybercrime and its effects on corporate stock value", *Journal of Information, Communication and Ethics in Society*, Vol. 17 No. 1, pp. 42-60. https://doi.org/10.1108/JICES-02-2018-0010

Victoire, T. A., Vasuki, M., Karunamurthy, A., Soundarya, D., & Sarumathi, S. (2023). A Survey on Cyber Security Threats and its Impact on Society. *International Journal of Research in Engineering, Science and Management*, *6*(6), 146–152. https://journal.ijresm.com/index.php/ijresm/article/view/2747

Wyatt, T. (2021). *Wildlife trafficking: A deconstruction of the crime, victims and offenders*: Springer.