Journal of Information Technology,
Cybersecurity, and Artificial Intelligence

(Review Article)

Counteracting Cybercrimes in Florida

Ahmed Al Zaidy

Information Technology Programs
Florida State College at Jacksonville
Jacksonville, Florida, United State of America

Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 2024, Volume 1, Issue 1

Publication history: Received on 26 October 2024; revised on 29 October 2024; accepted on 30 October 2024

Article DOI: https://doi.org/10.70715/jitcai.2024.1.1.001

Abstract

This article explores Florida's high rate of cybercrime and the efforts being made to combat it. Florida has the second-highest rate of cybercrime events in the United States, with significant financial losses. The most frequent dangers are call center frauds, ransomware, investment fraud, and business email compromise. Strong defense tactics, including multi-factor authentication, safe password policies, cybersecurity training, frequent software upgrades, network segmentation, and dependable backups, are emphasized throughout the text. It also emphasizes how important it is to have efficient incident response procedures, promote teamwork, and use continuous monitoring to lessen cyberthreats. The essay goes on to discuss the vital role that international collaborations and law enforcement play in the battle against cybercrime.

Keywords: Cybersecurity; Cybercrimes; threats; attacks.

1. Introduction

Florida is second only to California in terms of cybercrime events, with 42,792 recorded complaints totaling $844.9 million in losses, according to the 2022 Internet Crime Complaint Center (IC3) report [4].

The FBI's IC3 platform facilitates the reporting of suspected cybercrimes and unlawful acts aided by the internet by individuals. In 2000, the FBI and the National White Collar Crime Center (NW3C) collaborated to establish the IC3, which provides the public with a convenient means of reporting questionable online criminal activity [3].

800,944 complaints totaling over $10.3 billion in reported damages were filed with the IC3 in 2022. Financial losses grew by 49% while the number of complaints decreased by 5% [3].

Figure 1 illustrates the number of cybercrime victims by state. With 42,792 reported incidents, Florida is second to California with the most victims.

[*] Corresponding author: First Last Name

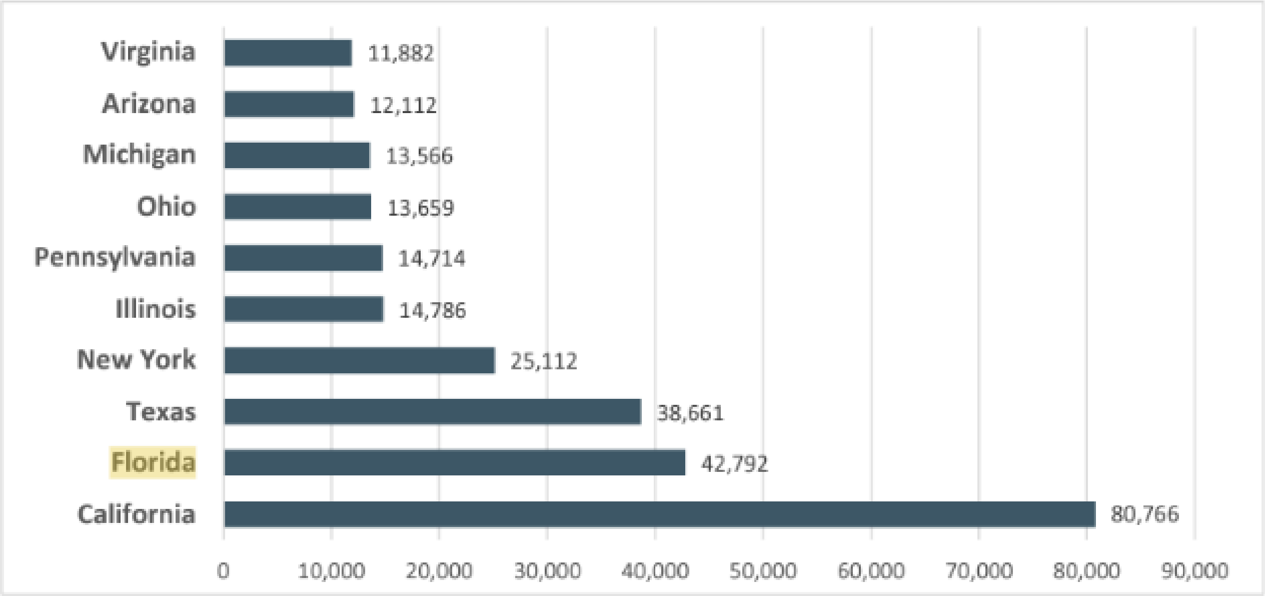


Figure 1 Cybercrime Victims by State [4]

Figure 2 shows the total financial losses per state from reported cybercrimes. Florida suffered $844.9 million in losses, while California exceeded $2 billion.

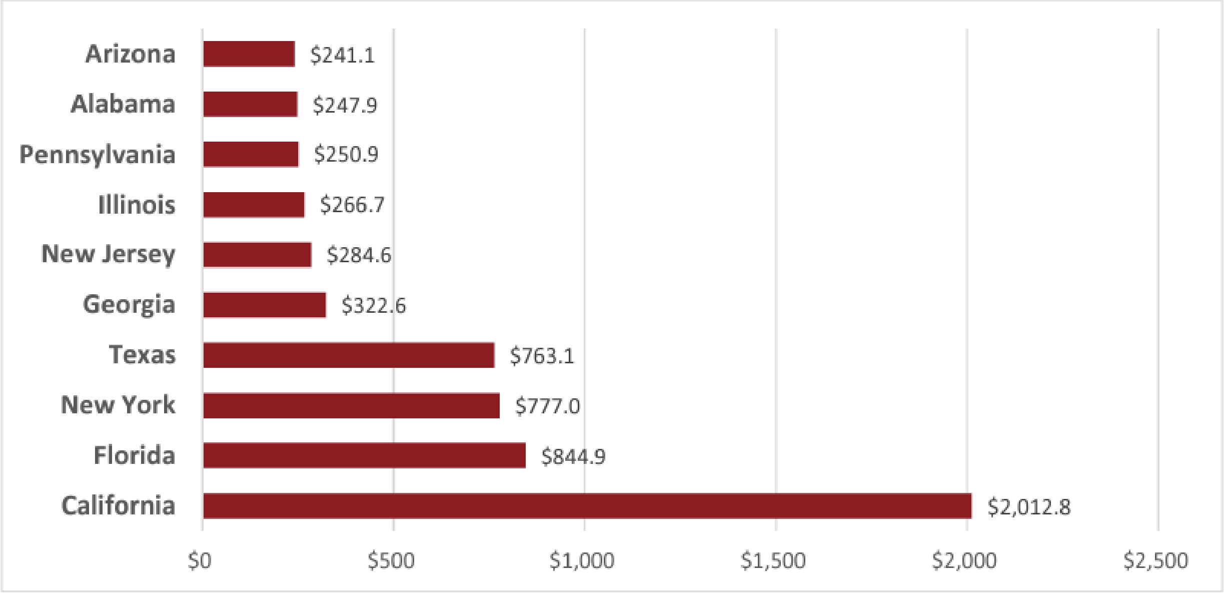


Figure 2 Total Financial Losses Per State [4]

Florida's cybercrime presents major hazards to a number of industries, including technology, insurance, and banking [6]. Law enforcement's involvement in preventing and looking into cyber events has changed as a result of the strain these crimes have placed on the criminal justice system [2]. The need for international cooperation is highlighted by the worldwide nature of cybercrime, which includes the dissemination of malicious software and the exploitation of computer systems [5]. Wide-ranging cooperation is necessary to address the intricate problems posed by cybercrime, and partnerships are essential to prevention [1].

The most common cyberthreats in 2022, according to IC3, were ransomware, contact center scams, investment fraud, and business email compromise (BEC).A. Email Compromise in Business (BEC) 21,832 complaints against BEC were received by IC3 in 2022; as a result, adjusted losses totaling over $2.7 billion were incurred. BEC is a sophisticated fraud that preys on companies and individuals that transact money. Through social engineering or hacking, unsanctioned parties obtain access to authentic company email accounts in order to enable illicit money transfers Fraudsters are always improving their BEC strategies; they are no longer limited to conventional email hacking and are now posing as vendors, asking W-2 data, and focusing on the real estate industry. The usage of cryptocurrency custodial accounts and phone spoofing of real company numbers to deceive victims into verifying fake banking details has increased recently. The prevalence of these strategies emphasizes how crucial it is to avoid fraud by using multi-factor authentication, calling potential victims directly instead of over email, and closely reviewing their email correspondence.

Fraudulent Investment Schemes Investment scams were the most expensive cybercrime in 2022. The amount of complaints increased by 127% from $1.45 billion in 2021 to $3.31 billion in 2022. The biggest contributor was fraud involving cryptocurrencies, which increased by 183% from $907 million in 2021 to $2.57 billion in 2022. There have been a number of scams involving cryptocurrency investments that have surfaced. These include liquidity mining, in which victims connect their wallets to fraudulent platforms and lose money, and impersonation scams in which real estate agents or celebrities offer fictitious investment opportunities. The financial losses from investment frauds that were reported to IC3 are shown in Figure 3.

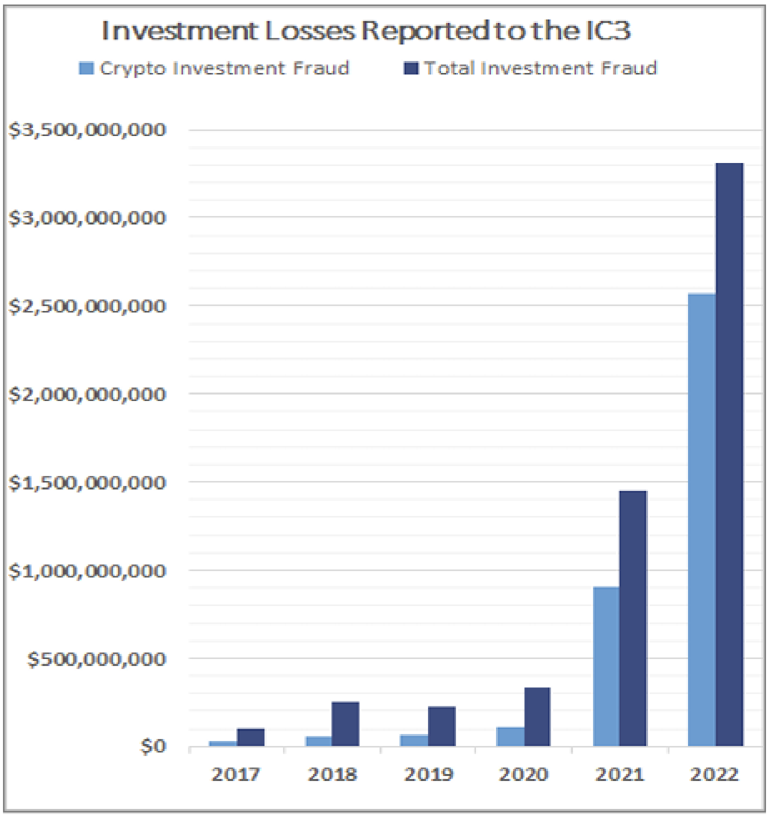


Figure 3 The Financial Losses from Investment Scams [4]

Malware IC3 received 2,385 ransomware complaints in 2022, resulting in losses of $34.3 million. Malicious software is used in ransomware attacks to encrypt victims' data, after which the cybercriminal demands a fee to unlock the data. Data often remains unreadable if the ransom is not paid. Attackers may not just encrypt data; they might also exfiltrate it and disseminate it if they don't receive the ransom. The major ways that ransomware is still infected are through phishing emails, RDP exploitation, and software flaws. Preventing ransomware attacks requires regular software upgrades, user education, and secure remote desktop protocol (RDP) access. Reports from IC3 indicate that in 2022, ransomware outbreaks affected 14 out of 16 critical infrastructure sectors. Figure 4 shows the sectors that the malware has affected.

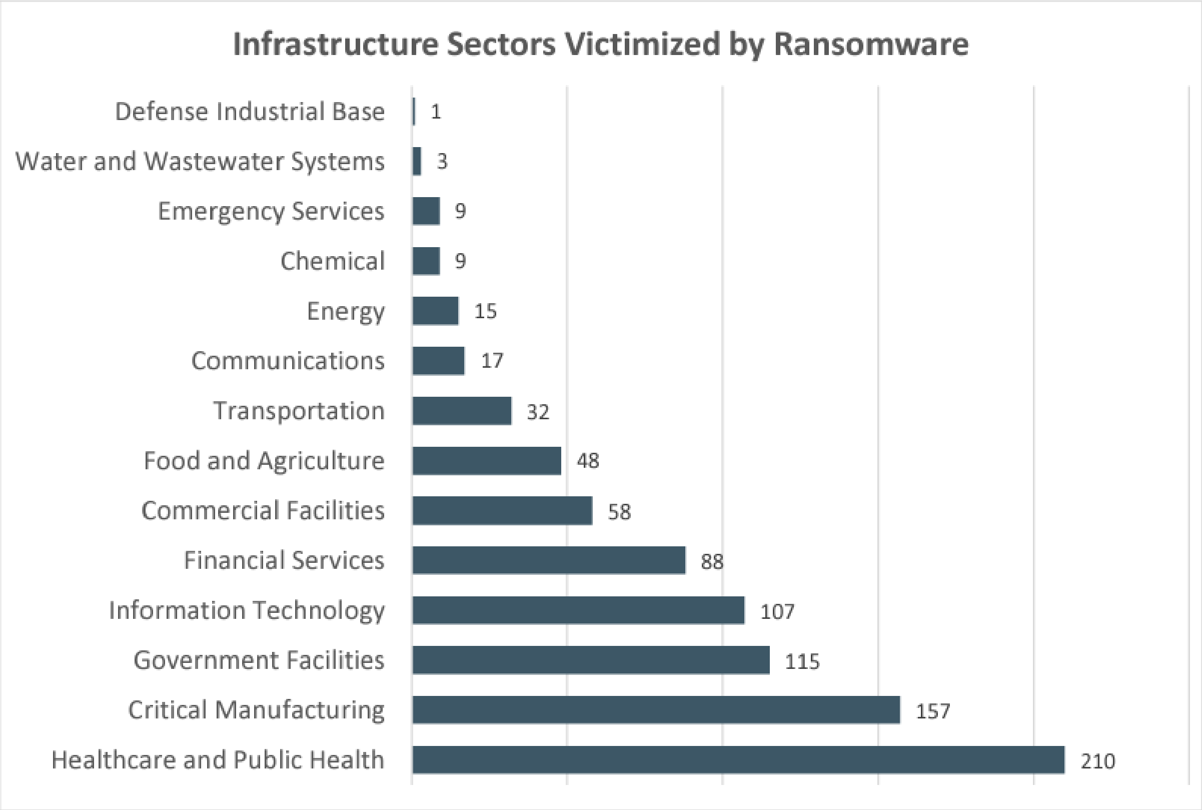
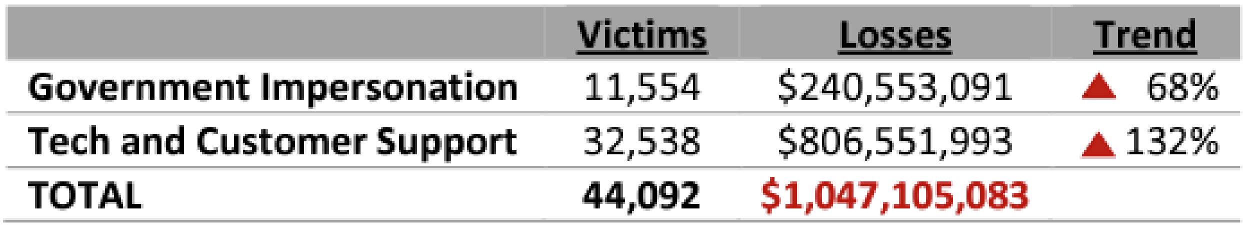


Figure 4 Sectors Impacted by Ransomware [4]

Fraud in Call Centers Elderly victims are the main target of call center fraud; 46% of victims are over 60, and they accounted for 69% of the overall losses, which exceeded $724 million in 2022. South Asia, and especially India, is where these scams most frequently start. In response, Indian law enforcement has joined up with the FBI and the Department of Justice (DOJ) to combat these scams. Due to this cooperation, multiple searches, arrests, and disruptions of call centers engaged in these fraudulent activities took place in 2022. The number of victims of call center fraud and their monetary losses are displayed in Figure 5.



	Victims	Losses	Trend
Government Impersonation	11,554	$240,553,091	▲ 68%
Tech and Customer Support	32,538	$806,551,993	▲ 132%
TOTAL	**44,092**	**$1,047,105,083**	

Figure 5 Number of Call Center Fraud Victims [4]

2. COUNTERACTING CYBERCRIMES

Addressing cybercrimes requires a comprehensive, multi-layered approach that includes prevention, detection, and response strategies. The following are key measures and practices to mitigate cybercrime effectively:

2.1 Cybersecurity Training and Awareness

In the digital era, it is essential to emphasize the importance of cybersecurity awareness and training. This section provides an overview of the critical components of such programs, outlines common attack methods, and highlights the benefits of fostering a cybersecurity-conscious culture.

Basic Awareness: Introduce foundational concepts about common cyber threats like phishing, malware, and ransomware. Teach users about creating strong passwords and the risks of reusing them.

Ongoing Training: Conduct frequent training sessions to inform employees about emerging threats and best practices. Simulate phishing attacks to train employees on recognizing suspicious activities.

Establish Policies: Define clear policies covering acceptable use, data security, and incident response, ensuring employees understand their roles through continuous education.

Mobile Device Security: Train staff on securing mobile devices using encryption, strong authentication, and regular software updates.

Securing Remote Work: As remote work expands, guide employees on securing home networks and utilizing virtual private networks (VPNs) and multi-factor authentication (MFA).

Incident Response: Prepare employees to respond effectively to cyber incidents by promptly reporting and mitigating damage.

Up-to-date Resources: Ensure training materials reflect the latest cyber threats and technologies.

Fostering Security Culture: Promote a culture where all employees recognize their role in maintaining a secure environment.

I.T. Collaboration: Establish strong communication between technical staff and non-technical employees, encouraging reporting of suspicious activity.

Gamification: Incorporate interactive elements into training to enhance engagement.

2.2 Strong Password Policies

Strong password policies are essential for safeguarding sensitive information. Implementing such policies prevents unauthorized access and strengthens overall security:

Password Length: Set minimum lengths, typically starting at eight characters, and encourage using longer, more complex passphrases.

Complexity: Require combinations of upper and lowercase letters, numbers, and symbols to avoid easily guessable patterns.

Regular Expiration: Mandate password changes at intervals, commonly every 90 days.

Password History: Prevent users from reusing old passwords within a specific number of changes.

Account Lockout: Implement lockout policies after several failed login attempts to protect against brute-force attacks.

Two-Factor Authentication (2FA): Enforce 2FA to add a security layer.

User Education: Educate users on creating secure passwords and avoiding phishing threats.

Password Storage: Use industry-standard methods such as hashing with salted algorithms to store passwords securely.

Monitoring and Auditing: Regularly audit user accounts to identify weak or compromised passwords.

Recovery Mechanisms: Implement secure password recovery options.

Security Assessments: Conduct regular assessments to identify weaknesses in password management.

Encryption: Encrypt communications related to password management to prevent interception.

Policy Enforcement: Use tools to ensure compliance with password policies.

2.3 Multi-Factor Authentication (MFA)

MFA enhances security by requiring multiple forms of identification before granting access to systems. By combining factors such as passwords (something you know), tokens (something you have), and biometrics (something you are), MFA mitigates the risks of relying solely on passwords.

2.4 Regular Software Updates and Patch Management

Keeping software updated is crucial for closing vulnerabilities. Regular updates provide new features and performance improvements and ensure systems are protected against the latest threats. Patching should be timely and prioritized based on criticality.

2.5 Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)

Firewalls and IDS/IPS are integral to network security. Firewalls control network traffic based on predefined rules, while IDS/IPS systems detect, alert, and block suspicious activity, adding multiple layers of protection.

2.6 Network Segmentation

Dividing a network into smaller segments restricts access to sensitive information, minimizes the impact of breaches, and helps contain threats. This reduces the attack surface and limits lateral movement within networks.

2.7 Regular Backups

Frequent backups are essential to recover data during hardware failure, corruption, or cyber-attacks. Automated solutions, offsite backups, and regular testing of recovery procedures help secure critical data.

2.8 Incident Response Plans

A well-designed incident response plan (IRP) enables organizations to manage cyber incidents effectively, minimizing damage, recovery time, and costs. Preparing the response team, monitoring for threats, and practicing containment are essential aspects of an IRP.

2.9 Collaboration and Information Sharing

Collaboration within the organization and with external entities enhances cyber defenses. Sharing information about threats and best practices fosters a proactive approach to addressing potential vulnerabilities.

2.10 Security Audits and Penetration Testing

Regular security audits ensure that policies and controls are effective. Penetration testing simulates cyber-attacks to identify and address vulnerabilities, making organizations more resilient against threats.

2.11 Data Encryption

Encryption protects sensitive information by converting it into an unreadable format, ensuring that even if data is intercepted, it cannot be accessed without the decryption key.

2.12 Endpoint Security

Endpoint security safeguards devices like computers and smartphones that connect to a network. Antivirus software, firewalls, and patch management prevent malware and unauthorized access to these endpoints.

2.13 User Access Control

User access control limits system access based on user roles and responsibilities. It ensures that users have only the permissions necessary to perform their jobs, reducing the risk of accidental or malicious data exposure.

2.14 Secure Development Practices

Adopting secure coding practices helps prevent vulnerabilities during software development. Regular testing, code reviews, and secure coding standards contribute to building secure applications.

2.15 Regulatory Compliance

Compliance with legal and industry standards, such as GDPR or HIPAA, ensures that organizations follow best practices for protecting sensitive data and avoiding legal and financial repercussions.

2.16 Cyber Insurance

Cyber insurance offers financial protection against the costs of data breaches and cyber-attacks. Policies often cover legal fees, notification costs, and financial losses from downtime or fraud.

2.17 Continuous Monitoring

Continuous monitoring provides real-time visibility into system activities, enabling organizations to quickly detect and respond to threats. This proactive approach helps prevent small incidents from escalating into significant breaches.

2.18 Phishing Awareness

Raising awareness about phishing helps employees recognize and avoid deceptive emails designed to steal sensitive information. Training, two-factor authentication, and regular updates are critical to reducing phishing risks.

2.19 Collaboration and Reporting

Effective collaboration and timely reporting of suspicious activities help organizations respond swiftly to potential threats, mitigating the impact of cyber incidents. When implemented together, these strategies create a robust defense framework against cybercrime.

3. Introduction

In 2022, Florida was second among the top ten states affected by cybercrime, with 42,792 reported cases and financial losses amounting to $844.9 million. The Internet Crime Complaint Center (IC3), a platform for reporting suspected internet-facilitated crimes, received 800,944 reports nationwide, resulting in over $10.3 billion in losses. With losses surpassing $2 billion, California was the only state to surpass Florida's total losses.

Cybercrime threatens various industries, including finance, insurance, and technology. The impact on the criminal justice system necessitates rethinking social response mechanisms and the evolving role of law enforcement in cybercrime prevention and investigation. The widespread nature of cybercrime further emphasizes the need for global cooperation to address these threats effectively. Cybercrime threats vary, including business email compromise (BEC), investment fraud, ransomware, and call center scams.

BEC is a highly sophisticated scam aimed at businesses and individuals involved in financial transactions, where cybercriminals gain unauthorized access to legitimate email accounts via techniques like social engineering or hacking. The nature of BEC attacks has shifted from simple email spoofing or hacking to more complex fraudulent activities, such as creating fake bank accounts. In 2022, many attacks focused on investment accounts rather than traditional banking accounts. One common technique involves cybercriminals spoofing legitimate business phone numbers to deceive victims into confirming fraudulent transactions.

To combat cybercrime, it is critical to establish secure verification procedures for payments and purchasing requests outside email communications. This includes direct phone confirmations using verified contact details. Best practices include carefully reviewing email addresses, links, and the contents of unsolicited communications, avoiding clicks on suspicious links or attachments, and verifying requests through trusted channels.

2022 IC3 reported a 127% spike in investment scams, with cryptocurrency-related fraud increasing dramatically from $907 million to $2.57 billion. The significant rise in crypto scams led to considerable financial losses, particularly affecting individuals aged 30 to 49. Common types of crypto-investment scams include liquidity mining fraud, hacked social media accounts, impersonation of celebrities, deceptive real estate deals, and fraudulent job offers.

Ransomware remained a critical threat in 2022, with 2,385 complaints leading to over $34.3 million in adjusted losses. Ransomware attacks typically encrypt the victim's data, rendering it unusable until a ransom is paid. Cybercriminals often exfiltrate sensitive data, threatening to release it if the ransom is not remitted. Ransomware infections often result from phishing emails, Remote Desktop Protocol (RDP) vulnerabilities, and software flaws.

IC3 advises regular operating system and software updates and conducts user training and phishing simulations to raise awareness of the dangers associated with suspicious emails, links, and attachments. If using RDP, organizations should ensure its security and implement continuous monitoring. Additionally, data backups should be stored offline to safeguard against ransomware attacks.

Call center fraud, which disproportionately targets elderly individuals, has become a growing concern. Almost 46% of the victims in 2022 were over 60, and they accounted for 69% of the total financial losses, totaling over $724 million. In response, the U.S. Department of Justice and the FBI have partnered with Indian law enforcement agencies to combat transnational call center fraud. This collaboration led to multiple raids in 2022, dismantling the fraudulent network and preventing further attacks.

References

[1] Caneppele, S., & Silva, A. d. (2022). Cybercrime. doi:https://doi.org/10.4337/9781839106385.00024

[2] Farrell, G., & Birks, D. (2018). Did cybercrime cause crime to drop? Crime Science, 7(1). doi:doi: 10.1186/S40163-018-0082-8

[3] FBI. (2023, March 22). Internet Crime Complaint Center Releases 2022 Statistics. Retrieved from fbi.gov: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

[4] IC3. (n.d.). Internet Crime Report 2022. Retrieved from ic3.gov: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[5] Kirwan, G., & Power, A. (2013). Cybercrime: Psychology of cybercrime.

[6] Suja, P., & Raghavan, N. (2013). cybercrime in the banking sector. International journal of research in social sciences, 4(1), 189-194.