WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

"Combating Digital Arrest: Cybersecurity Measures to Safeguard Customers from Coercive Online Tactics."

DIVYANSH MITRA[1], DR. SNIGDHA SINGH [2]

[1] (Student, Amity Business School, Amity University, Lucknow, Uttar Pradesh)
[2] (Assistant Professor, Amity Business School, Amity University, Lucknow, Uttar Pradesh)

ABSTRACT :

This paper explores the rise of coercive online tactics—such as phishing, digital arrest scams, and SIM swapping—that are increasingly used to target and exploit unsuspecting customers. With the exponential growth of digital connectivity, these threats have evolved to exploit human psychology and systemic vulnerabilities. The study uses a qualitative approach grounded in secondary research to analyze real-world cases and highlight the gaps in cybersecurity awareness and infrastructure. Key findings reveal low adoption of safety practices like multi-factor authentication, making users vulnerable to identity theft and financial fraud. The paper concludes with five actionable recommendations: strengthening public awareness, mandating security protocols, enhancing government-industry collaboration, deploying AI-based monitoring, and investing in cybersecurity training. Together, these strategies form a holistic defense mechanism against digital coercion and are essential for securing the trust and safety of online users.

1. Introduction

With the digital era progressing rapidly, cyber threats have evolved in both scale and sophistication. Among these, coercive online tactics—such as phishing, ransomware attacks, digital arrest scams, and impersonation fraud—pose a direct threat to customers' safety and trust. These malicious tactics often manipulate users emotionally or psychologically to gain access to sensitive data or financial assets. The significance of this research lies in its focus on identifying these coercive practices and formulating robust cybersecurity measures tailored to protect the end-user.

Key Objective: To analyze the growing menace of coercive online tactics and propose pragmatic cybersecurity interventions to safeguard customers from digital exploitation.

2. Review of Literature

Academic literature has highlighted the dual challenge of technological loopholes and low cyber literacy among the public. Anderson (2020) in "Security Engineering" explores the vulnerabilities in system design that hackers often exploit, while Brenner (2018) focuses on how online threats affect individual users psychologically. Reports from institutions like Norton and McAfee underline a rising trend of digital extortion, especially among users unfamiliar with cybersecurity protocols.

Themes Identified:

- The rapid evolution and diversification of cyber threats
- Consumer behavior as a determining factor in vulnerability
- Response frameworks developed by government and private sectors

3. Research Methodology

The research follows a qualitative approach and relies primarily on secondary data collection. Various academic journals, case studies, government reports (CERT-In), and white papers from cybersecurity firms form the backbone of this study. A comparative analysis was conducted between cybersecurity practices in India and other developed countries, helping to identify the gaps in customer education and digital infrastructure.

4. Objectives of the Study

- **To define and categorize coercive online tactics:** Understanding various types such as phishing, SIM swapping, digital arrest scams, and their psychological manipulation techniques.

- **To examine the short-term and long-term impact on customers:** Assessing financial losses, identity theft, emotional trauma, and trust erosion in digital services.
- **To evaluate the existing cybersecurity ecosystem:** Studying the readiness and effectiveness of cybersecurity frameworks in institutions, government agencies, and user-level practices.
- **To suggest actionable cybersecurity measures:** Recommending feasible steps for different stakeholders to mitigate risks, including public awareness, tech-based tools, and regulatory interventions.

5. Data Analysis

Data collected from various cybercrime surveys revealed the alarming frequency and success rate of coercive tactics:

Key Findings:

- Over 65% of individuals reported receiving suspicious emails designed to steal credentials (phishing).
- 40% admitted they do not verify suspicious links or sender details.
- Only 30% of users had multi-factor authentication enabled on critical accounts.

Case Studies (in Points):

1. **Digital Arrest Scam (India, 2020):**
    - Fraudsters impersonated law enforcement officers.
    - Victims were told they were involved in legal crimes.
    - Threatened with arrest unless they transferred money.
    - Used spyware and spoofed caller IDs to manipulate victims.
2. **Phishing Campaign Targeting Senior Citizens (Global):**
    - Emails mimicked health agencies during the COVID-19 pandemic.
    - Contained malicious links asking for bank details or health insurance information.
    - Resulted in identity theft and financial fraud.
3. **SIM Swap Fraud (India and US):**
    - Attackers gained control of victims' phone numbers by bribing telecom staff.
    - Used OTPs received on the swapped SIM to access bank and UPI accounts.
    - Several victims lost lakhs of rupees within minutes.

6. Recommendations

1. **Public Awareness Campaigns:** Launch widespread awareness programs using mass media to educate citizens about phishing emails, spoofed URLs, and scam calls. Digital literacy should be integrated into school curriculums and community education programs.
2. **Mandatory Multi-Factor Authentication (MFA):** Regulatory authorities should require all financial and high-risk digital platforms to implement MFA, which significantly reduces the success of unauthorized access.
3. **Government Collaboration:** National helplines, local cybercrime reporting portals, and cyber cells should be made more accessible and responsive. Government partnerships with tech firms can also help track and dismantle scam operations.
4. **AI-Based Fraud Detection Systems:** Financial institutions and e-commerce platforms should adopt AI-powered monitoring tools that detect unusual patterns and immediately alert customers to potential fraud.
5. **Training Programs:** Regular training sessions for bank employees, customer service agents, and even end-users can increase vigilance and reduce the risk of data breaches due to human error.

7. Conclusion

Cybersecurity is foundational to digital trust. As the threats continue to grow in complexity, both technological and human-centric solutions are required. Empowering customers with knowledge and implementing systemic safeguards are critical to creating a secure digital environment. By aligning public policy, corporate responsibility, and user awareness, a holistic defense against coercive cyber tactics can be built.

8. REFERENCES (SELECTED)

1. Anderson, R. (2020). *Security Engineering*.
2. Brenner, S. (2018). *Cybercrime: Criminal Threats in Cyberspace*.
3. Norton Cybersecurity Insights Report (2022).
4. CERT-In Annual Reports.