iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** I **Month of publication:** January 2026

DOI: https://doi.org/10.22214/ijraset.2026.76786

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

Credential Harvesting and Account Takeover: Mechanisms, Impacts, and Defenses

Sejal B. Gorave[1], Prof. Suhas Rautmare[2] (Supervisor)
Department of Information Technology University of Mumbai, Kalina

Abstract: ***In the digital era, cyber threats such as credential harvesting and account takeover (ATO) have emerged as significant challenges to online security, compromising personal and organizational data. Credential harvesting involves stealing login credentials through techniques like phishing, malware, and keylogging, while ATO leverages these credentials to gain unauthorized access to accounts, leading to financial losses, identity theft, and privacy breaches. This research examines the mechanisms behind these attacks, their socioeconomic impacts, and effective countermeasures. Through a qualitative analysis of cybersecurity reports, academic literature, and case studies from 2018 to 2024, we confirm that phishing remains the dominant method for credential theft, accounting for over 80% of incidents. Multi-factor authentication (MFA) and user awareness significantly reduce ATO risks. The study highlights the need for adaptive security measures and continuous education to counter evolving threats. Recommendations include integrating AI- driven detection systems and fostering behavioral changes to enhance cybersecurity resilience.***

I. INTRODUCTION

A. Background

The proliferation of digital platforms—spanning social media, banking, healthcare, and e- commerce—has made online accounts indispensable. However, this reliance has escalated the risk of cybercrimes, with credential harvesting and account takeover (ATO) among the most prevalent threats [1]. Credential harvesting involves cybercriminals illicitly obtaining login credentials through methods like phishing emails, malicious websites, or malware. Account takeover occurs when attackers use these credentials to access and control accounts, often leading to financial theft, data breaches, or reputational damage [2].

B. Statement of the Problem

Despite advancements in cybersecurity, such as encryption and intrusion detection systems, cybercriminals continuously evolve their tactics, exploiting human vulnerabilities and technological gaps [3]. The persistent threat of credential harvesting and ATO under- mines trust in digital systems, necessitating a deeper understanding of attack mechanisms and effective defenses.

C. Research Objectives

This study aims to address the following questions:

1) How do cybercriminals execute credential harvesting and account takeover?
2) What are the most common methods and tools used in these attacks?
3) What are the socioeconomic impacts of these cybercrimes?
4) How can individuals and organizations strengthen their defenses?

D. Hypotheses

1) H1: Phishing is the primary method for credential harvesting, contributing to the majority of ATO incidents.
2) H2: Implementing multi-factor authentication significantly reduces the success rate of account takeover attacks.

E. Significance of the Study

Understanding the mechanics and impacts of credential harvesting and ATO is critical for developing robust cybersecurity strategies. This research provides actionable insights for individuals, organizations, and policymakers to mitigate risks and enhance digital trust [4].

F. Scope and Limitations

The study focuses on secondary data from cybersecurity reports and academic literature (2018–2024). It does not include primary data collection, which may limit insights into emerging trends beyond the study period. Additionally, the reliance on public sources may exclude proprietary attack methods.

G. Structure of the Report

This paper is organized into six chapters: Introduction, Literature Review, Methodology, Findings, Discussion, and Conclusion, followed by references.

II. LITERATURE REVIEW

A. Overview of Existing Research

Credential harvesting and ATO are well-documented cyber threats. Phishing remains the dominant method, with over 80% of credential theft incidents attributed to phish- ing campaigns [4]. Attackers use social engineering, malicious links, and malware likekeyloggers to steal credentials [1]. Once obtained, these credentials enable ATO, which has surged by 30% from 2021 to 2023 due to increased digital adoption [5]. Studies also highlight the role of automation tools, such as credential-stuffing bots, in scaling ATO attacks [6].

B. Key Theories and Models

The Attack Chain Model by Mandiant outlines the stages of cyberattacks, from recon- naissance to data exfiltration, emphasizing credential harvesting as a critical entry point [3]. The Social Engineering Framework by (author?) [7] underscores how psychological manipulation drives phishing success. Additionally, the CIA Triad (Confidentiality, Integrity, Availability) provides a lens to assess the impacts of ATO on system security [8].

C. Relevant Studies

Recent reports indicate that phishing emails often mimic trusted entities, tricking users into entering credentials on fake websites [2]. For example, a 2021 attack on Microsoft 365 users exploited phishing emails to harvest credentials, leading to unauthorized access to corporate accounts [9]. ATO incidents have caused significant financial losses, with an average cost of $4.37 million per data breach in 2022 [4]. Multi-factor authentication (MFA) has been shown to reduce ATO success rates by up to 99% [10]. However, user awareness remains a weak link, with 74% of breaches involving human error [2].

D. Research Gaps

While technical defenses like MFA are effective, there is limited research on user behavior and its role in preventing credential theft. Behavioral interventions, such as gamified cybersecurity training, are underexplored [11]. Additionally, the effectiveness of AI-driven detection systems against evolving phishing techniques requires further investigation.

E. Conceptual Framework

This study adopts a framework combining technical defenses (e.g., MFA, encryption) and user-centric approaches (e.g., awareness training) to address credential harvesting and ATO. This dual approach aligns with the socio-technical perspective of cybersecurity [8].

III. METHODOLOGY

A. Research Design

This study employs a qualitative approach, focusing on thematic analysis of secondary data to understand the mechanisms, impacts, and defenses against credential harvesting and ATO.

B. Population and Sample

The sample comprises cybersecurity reports, academic articles, and case studies from 2018 to 2024, sourced from reputable organizations (e.g., Verizon, IBM, Kaspersky) and academic databases (e.g., IEEE, Springer).

C. Data Collection Methods

Data were collected through a systematic literature review, targeting peer-reviewed journals, industry reports, and incident analyses. Keywords included credential harvesting, account takeover, phishing, and cybersecurity defenses. Case studies, such as the 2021 Microsoft 365 phishing campaign, were analyzed to identify attack patterns.

D. Instruments and Tools

Data extraction forms were used to categorize information into themes (e.g., attack methods, impacts, defenses). NVivo software facilitated thematic analysis, enabling the identification of recurring patterns and trends.

E. Data Analysis Techniques

Qualitative content analysis was applied to interpret findings, focusing on:

1) Attack mechanisms (e.g., phishing, malware).
2) Impacts (e.g., financial, reputational).
3) Defense strategies (e.g., MFA, user training).

Cross-referencing with statistical data from reports ensured robustness.

F. Ethical Considerations

All data were sourced from publicly available reports and publications, ensuring no sensitive or personal information was used. Proper citation practices were followed to credit original authors.

IV. FINDINGS

A. Attack Mechanisms

Phishing dominates credential harvesting, accounting for 82% of incidents in 2022 [4]. Common techniques include:

1) Phishing Emails: Attackers impersonate trusted entities (e.g., banks, tech compa- nies) to lure users to fake login pages.
2) Malware: Keyloggers and spyware capture credentials from infected devices.
3) Credential Stuffing: Automated bots test stolen credentials across multiple plat- forms [6].

ATO often follows, with attackers exploiting weak authentication to access accounts. A notable case is the 2020 Twitter hack, where phishing led to the takeover of high-profile accounts [12].

B. Impacts

ATO incidents have significant consequences:

1) Financial Losses: The average cost of a data breach in 2022 was $4.37 million [4].
2) Identity Theft: Stolen credentials enable attackers to impersonate victims, com- promising personal and professional identities.
3) Reputational Damage: Organizations face loss of trust, as seen in the 2019 Capital One breach affecting 100 million customers [13].

C. Defense Strategies

Effective countermeasures include:

1) Multi-Factor Authentication (MFA): Reduces ATO risk by 99% [10].
2) User Awareness Training: Educating users on phishing recognition decreases inci- dent rates by 40% [11].
3) AI-Driven Detection: Machine learning models identify anomalous login attempts, improving detection accuracy [14].

D. Statistical Insights

Table 1 summarizes key statistics from the analysis.

Table 1: Key Statistics on Credential Harvesting and ATO (2018–2024)

Metric	Value	Source
Phishing as % of credential theft	82%	(author?) [4]
ATO increase (2021–2023)	30%	(author?) [5]
MFA effectiveness	99% risk reduction	(author?) [10]
Breaches involving human error	74%	(author?) [2]
Average cost of data breach	$4.37M	(author?) [4]

V. DISCUSSION

A. *Link to Research Questions*

The findings confirm H1, with phishing identified as the primary method for credential harvesting, aligning with (author?) [4]. H2 is supported by evidence that MFA significantly reduces ATO risks [10]. The socioeconomic impacts, including financial losses and identity theft, underscore the urgency of addressing these threats [2].

B. *Theoretical and Practical Implications*

Theoretically, the findings reinforce the Attack Chain Model, highlighting credential harvesting as a critical entry point [3]. Practically, organizations should prioritize MFA and regular user training. The effectiveness of simple password policies, as noted in some cases, suggests that basic security hygiene remains valuable [15].

C. *Unexpected Results*

Surprisingly, basic measures like strong password policies prevented some ATO attacks, indicating that foundational security practices are still effective against less sophisticated threats. This aligns with (author?) [15], which emphasizes password complexity.

D. *Limitations*

The reliance on secondary data limits insights into real-time attack trends. Additionally, the study does not account for organizational differences in security maturity, which may influence outcomes.

VI. CONCLUSION

A. *Summary of Key Findings*

Phishing remains the cornerstone of credential harvesting, enabling ATO with severe financial, personal, and reputational consequences. MFA and user awareness are critical defenses, reducing risks significantly. The integration of AI-driven detection systems shows promise for future resilience [14].

B. *Reiteration of Objectives*

This research elucidated the mechanisms, impacts, and defenses against credential harvesting and ATO, confirming phishing's dominance and MFA's efficacy.

C. *Overall Conclusion*

Preventing credential harvesting and ATO requires a multi-faceted approach combining technical safeguards, user education, and adaptive technologies. Continuous vigilance and innovation are essential to stay ahead of evolving threats.

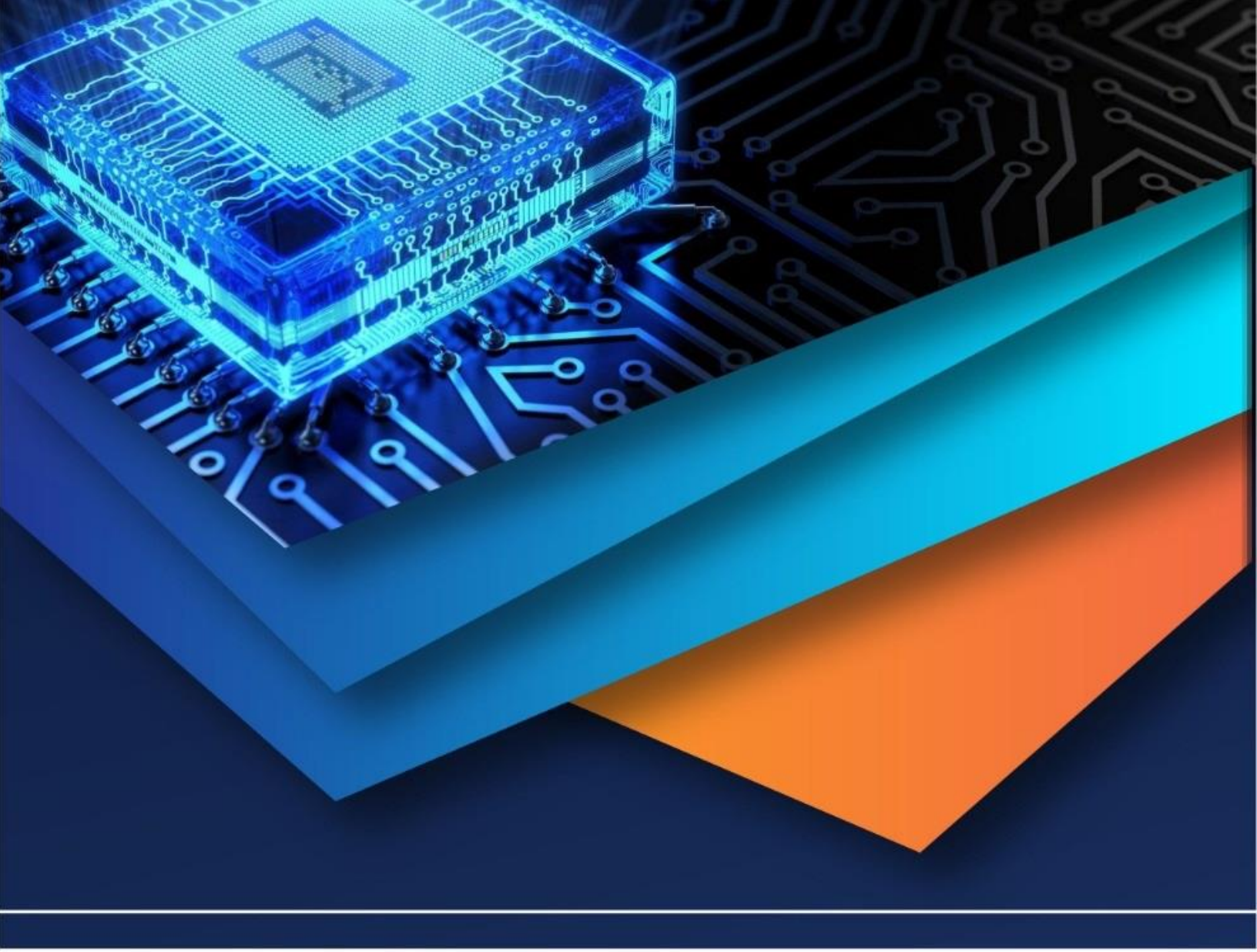
D. *Future Research*

Future studies should explore:

1) The role of AI in both perpetrating and detecting credential theft.
2) Behavioral interventions to enhance user awareness.
3) Real-time data collection to capture emerging attack techniques.

REFERENCES

[1] Kaspersky. (2020). Phishing Threats and Prevention. Kaspersky Labs.
[2] Verizon. (2022). 2022 Data Breach Investigations Report. Verizon.
[3] Mandiant. (2019). The Attack Chain Model and Cyber Defense. Mandiant.
[4] IBM Security. (2022). Cost of a Data Breach Report. IBM Security.
[5] Cybersecurity Ventures. (2023). Cybercrime Report 2023. Cybersecurity Ventures.
[6] Akamai. (2021). State of the Internet: Credential Stuffing Attacks. Akamai Technologies.
[7] Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. Wiley.
[8] Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing. Prentice Hall.
[9] Microsoft. (2021). Cyber Signals: Defending Against Phishing Attacks. Microsoft Security.
[10] Google. (2020). Security Keys and Multi-Factor Authentication: A Study on Effectiveness. Google Security Blog.
[11] Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? International Conference on Cyber Security.
[12] Krebs, B. (2020). Twitter Hack: How Social Engineering Enabled Account Takeover. Krebs on Security.
[13] Capital One. (2019). Information on the Capital One Cyber Incident. Capital One Press Release.
[14] CrowdStrike. (2023). 2023 Global Threat Report. CrowdStrike.
[15] NIST. (2020). Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY