Cybersecurity Threats through Phishing Attacks Targeting Internal Staff, Mitigation and Prevention

by Layanan Digital

Submission date: 07-Jan-2025 02:20PM (UTC+0700)
Submission ID: 2560561240
File name: IJAREEIE_Paper_-_Justinus_Andjarwirawan.pdf (1.67M)
Word count: 4098
Character count: 26010

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312001 |

Cybersecurity Threats through Phishing Attacks Targeting Internal Staff, Mitigation and Prevention

Justinus Andjarwirawan, Leo Willyanto Santoso, Kartika Gunadi

Informatics, Petra Christian University, Surabaya, Indonesia
Informatics, Petra Christian University, Surabaya, Indonesia
Informatics, Petra Christian University, Surabaya, Indonesia

ABSTRACT: Phishing attacks continue to be a predominant threat in the cybersecurity landscape, particularly when targeting internal staff to gain unauthorized access to internal systems. This paper explores how phishing attacks exploit human vulnerabilities, leading to significant security breaches. By analyzing real-world case studies like the recent Indodax case, the paper highlights the impact of phishing attacks on organizational security and explores the mitigation and prevention strategies that can be employed to reduce the risk of such attacks. Recent approaches, including employee training, advanced email filtering, and multi-factor authentication (MFA), are discussed, supported by current academic and industry research.

KEYWORDS: Phishing attacks, cybersecurity, internal staff, mitigation, prevention, security awareness.

I.INTRODUCTION

Phishing is one of the most pervasive attack vectors used by cybercriminals to compromise organizational security. Phishing attacks involve tricking individuals into divulging sensitive information, such as usernames, passwords, or other credentials, by posing as legitimate entities through email, social media, or other communication channels. These attacks often target internal staff, exploiting their trust to gain unauthorized access to internal systems.

Despite advancements in technical defences, phishing remains a significant threat because it targets human weaknesses rather than system vulnerabilities. In recent years, organizations across various industries have experienced devastating breaches caused by phishing attacks aimed at internal employees. These breaches can lead to financial loss, data theft, reputational damage, and even regulatory penalties.

This paper aims to examine the impact of phishing attacks on internal staff, provide notable case studies, and recommend actionable strategies for mitigating and preventing these attacks.

II.RESEARCH METHODS

The research methods utilized to examine the impact of phishing on internal staff, focusing on case studies such as the 2024 Indodax breach. It covers the selection of frameworks like ISO 27001 and COBIT for security integration and highlights how these methods contribute to understanding and mitigating cybersecurity risks.[1]

2.1 Research Approach

A mixed-methods approach was employed to gather both qualitative and quantitative data on phishing attacks targeting internal systems. The approach combined:

- Case Study Analysis: The Indodax breach and other high-profile incidents were used as case studies to explore the real-world impact of phishing on organizational systems. These case studies provide insight into how phishing campaigns penetrate defenses and exploit vulnerabilities in internal staff security awareness and technical systems.
- Survey of Best Practices: Through the analysis of ISO 27001[2] and COBIT[3] frameworks, the research examined how these globally recognized standards mitigate risks and enhance security defenses. The study also reviewed

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312001 |

scholarly literature and technical white papers to understand how organizations apply these frameworks to cybersecurity.

- Data Analytics: Reports from blockchain security companies such as PeckShield, Cyvers, and SlowMist were evaluated to understand the technical breakdown of the Indodax hack. This provided detailed evidence of the attack vectors and the effectiveness of security measures in place.

2.2 Case Study Selection

The selection of the Indodax breach as a case study is based on several factors:

- Relevance to Cryptocurrency Security: As the largest exchange in Indonesia, Indodax plays a key role in the regional crypto market, and its breach highlights vulnerabilities specific to digital assets.
- Significant Financial Impact: With $22 million stolen, this breach exemplifies the high financial stakes in cybersecurity and the evolving nature of cyber threats targeting exchanges.
- Phishing Techniques: The breach's phishing elements, particularly in targeting internal staff through spear-phishing, are highly relevant to the research focus on phishing-induced security incidents.

2.3 Data Collection

Data was gathered from a variety of sources:

- Primary Data: Interviews with cybersecurity experts who investigated the Indodax breach were conducted to gain first-hand insights into how phishing played a role in the attack. Employees from Indodax and security firms involved in the post-breach investigation were also consulted.
- Secondary Data: Security reports from third-party blockchain security firms like SlowMist and Cyvers provided detailed technical documentation of the attack's methodology. In addition, academic papers and industry reports on phishing mitigation techniques were analyzed to understand broader trends.
- Publicly Available Reports: Media reports, public statements from Indodax, and findings from blockchain research firms were integrated into the research for a holistic view of the incident.

2.4 Data Analysis

- Qualitative Analysis: Thematic analysis was conducted to identify key patterns in how phishing attacks are carried out and how internal staff typically respond. This method provided a deep understanding of organizational weaknesses and potential areas for improvement.
- Quantitative Analysis: Data from security reports and blockchain transaction analyses was used to quantify the financial impact of phishing-related breaches. The use of quantitative data enabled a clearer understanding of the scope of the problem.[4][5]

2.5 Framework Analysis

The integration of ISO 27001 and COBIT frameworks was evaluated through:

- Documentary Analysis: These frameworks were analyzed for their specific controls and processes related to phishing defense, incident management, and risk assessment. This approach helped assess the efficacy of these frameworks in real-world application.
- Comparative Analysis: The results of the Indodax case were compared against the expected outcomes had ISO 27001 and COBIT been fully implemented at the time of the breach. This comparison highlights the potential benefits of these frameworks for mitigating phishing attacks.

2.6 Testing the Security Framework

The research also includes testing the effectiveness of a security framework based on ISO 27001 and COBIT to mitigate phishing attacks. Simulated phishing campaigns targeting internal staff, alongside penetration testing and vulnerability assessments, were conducted to identify how effectively these frameworks protect against similar threats. This testing provided data on the real-world efficacy of integrating structured cybersecurity frameworks.

By combining qualitative and quantitative methods, the research provides a comprehensive examination of phishing-induced cyber threats, exploring both organizational vulnerabilities and defense mechanisms.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312001 |

III.PHISHING ATTACKS CASE STUDIES

Phishing attacks rely on social engineering tactics, where attackers impersonate legitimate individuals or entities to deceive the victim into providing access to sensitive systems. These attacks come in various forms:

- Email phishing: The most common type, where attackers send fraudulent emails designed to look legitimate.
- Spear phishing: A targeted form of phishing where attackers customize the message based on research about the victim, making it more convincing.
- Whaling: A subset of spear phishing, focusing on high-ranking individuals such as executives (CEO fraud).
- Clone phishing: Where a legitimate email is duplicated and slightly altered to include malicious links or attachments.

By targeting internal staff, attackers often aim to gain access to company credentials, escalate privileges, and infiltrate deeper systems.

3.1 Why Internal Staff Are Targets

Internal staff are often the weakest link in the security chain. While companies invest in firewalls, encryption, and anti-virus software, they sometimes overlook the importance of employee education and awareness. Staff might not recognize the signs of phishing, particularly when attacks are highly personalized or sophisticated. Employees with privileged access to internal systems, such as IT administrators, finance officers, and executives, are especially appealing targets due to the elevated access their credentials provide.

3.2 Notable Case Studies

3.2.1 Case Study 1: Sony Pictures (2014)

In 2014, a major cyberattack on Sony Pictures, attributed to the group known as the "Guardians of Peace," resulted in the exfiltration of sensitive data, including unreleased films, employee information, and internal emails. The attackers used phishing emails to gain access to internal systems. Once inside, they were able to move laterally, steal sensitive data, and cripple Sony's infrastructure. This breach not only resulted in financial loss but also damaged Sony's reputation and led to legal ramifications.

3.2.2 Case Study 2: Ubiquiti Networks (2021)

In January 2021, Ubiquiti Networks suffered a security breach through a phishing attack that targeted employees with administrative access to corporate IT systems hosted on third-party cloud providers. The attackers tricked the staff into revealing their credentials, allowing unauthorized access to Ubiquiti's internal system. This breach potentially exposed customer data, leading to loss of trust and a severe impact on the company's market value.

3.2.3 Case Study 3: Colonial Pipeline (2021)

The Colonial Pipeline ransomware attack in May 2021, which disrupted gas supplies across the eastern United States, also had phishing elements. Although the primary attack vector was through a compromised VPN account, phishing emails played a role in stealing the credentials of an employee who had access to sensitive internal systems. The breach led to critical infrastructure disruptions and heightened awareness of phishing's impact on national security.

3.2.4 Case Study: Indodax Phishing Attack (2020)

Indodax, Indonesia's largest cryptocurrency exchange, became a high-profile target of phishing attacks in 2020. As a leading platform for trading digital assets, Indodax was particularly attractive to cybercriminals seeking to steal cryptocurrency by gaining unauthorized access to user accounts through phishing attacks aimed at both internal employees and customers.

In the 2020 Indodax case, the phishing attack began with fake emails purporting to come from Indodax's official support team. These emails were designed to look legitimate, mimicking the company's branding and communication style. The emails instructed recipients—both employees and users—to click on a link that redirected them to a fake Indodax login page. The phishing website was nearly identical to the actual platform, tricking victims into entering their login credentials.

Once the attackers obtained these credentials, they gained access to users' accounts, where they could initiate unauthorized transactions. In the case of Indodax employees, those with privileged access to sensitive systems were targeted in spear-phishing attempts, which aimed to compromise the platform's internal systems and security protocols.

Though the exact number of victims was not disclosed, it was reported that several users fell prey to the phishing attack, resulting in financial losses. Some users lost access to their cryptocurrency holdings, as the attackers transferred

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312001 |

assets to external wallets, making it nearly impossible to recover. Although Indodax's internal systems were not breached directly, the attack highlighted the vulnerabilities associated with phishing attempts targeting both external users and internal staff.

The incident had a significant reputational impact on Indodax, causing concerns about the platform's security and the safety of its users' funds. The exchange responded by tightening its security protocols and issuing warnings to its user base, urging them to be more vigilant against phishing attacks.

Following the attack, Indodax implemented several measures to mitigate future phishing risks:

- Strengthened Customer Communication: Indodax improved its communication practices by warning users to verify email authenticity and avoid clicking on links in unsolicited emails. The company issued multiple security advisories and reminders to educate users on identifying phishing attempts.
- Multi-Factor Authentication (MFA): The exchange made MFA mandatory for all users. Even if a phishing attack was successful in obtaining login credentials, MFA provided an additional layer of security that made it significantly more difficult for attackers to access accounts without a secondary authentication method, such as a time-sensitive code sent to the user's mobile device.
- Enhanced Email Filtering: Indodax upgraded its email filtering systems to detect phishing attempts and block malicious emails before they reached employees or users. Advanced anti-phishing technologies were introduced to scan for indicators of fraudulent emails and prevent them from being delivered.
- Phishing Awareness Campaigns: To further mitigate the risk, Indodax conducted a series of security awareness campaigns for both employees and users. These campaigns included educational materials on how to recognize phishing attempts, report suspicious emails, and protect personal information.

3.2.5 Case Study: Indodax Phishing Attack (2024)

The Indodax 2024 phishing case [6][7] serves as an important lesson in the evolving nature of phishing threats, especially in industries dealing with high-value digital assets such as cryptocurrencies. It highlights the need for constant vigilance and layered security approaches that combine both user education and robust technical defenses. The implementation of MFA, in particular, proved to be a key defense mechanism against phishing attacks, offering protection even if credentials were compromised.

For organizations operating in high-risk industries, such as financial services and cryptocurrency trading, the case underscores the importance of continuously improving phishing defenses. It also demonstrates the need to integrate a governance framework, such as COBIT and ISO 27001, to manage security risks effectively and ensure that both technical and human vulnerabilities are addressed.

The 2024 Indodax breach serves as a prominent case study in cryptocurrency security vulnerabilities, where Indonesia's largest crypto exchange was hacked, resulting in the loss of around $22 million in various cryptocurrencies. The hacker managed to exploit weaknesses in Indodax's withdrawal systems, primarily targeting its hot wallets. Assets stolen included substantial amounts of Ethereum, Bitcoin, Tron, and Polygon, among others. This breach temporarily halted both the exchange's web and mobile applications as Indodax initiated an investigation and system maintenance.

Several blockchain security firms, including PeckShield, SlowMist, and Cyvers, flagged the breach shortly after it occurred. Cyvers reported over 150 suspicious transactions across multiple networks, with the stolen tokens being converted to Ethereum and laundered through crypto-mixing services like Tornado Cash. Experts, including Yosi Hammer from Cyvers, speculated that North Korea's infamous Lazarus Group could have been behind the attack, given the similarities in hacking techniques to other crypto heists attributed to the group.

In response, Indodax emphasized that customer balances were secure, even as they suspended services to contain the breach and assess the damage. However, this incident underscores the persistent threats to cryptocurrency exchanges, highlighting the importance of robust security measures, particularly against phishing and system exploitation attacks, which have become increasingly sophisticated.

The Indodax breach offers critical lessons for the implementation of security frameworks such as ISO 27001 and COBIT. By integrating these frameworks, crypto exchanges can manage risks more effectively and mitigate potential vulnerabilities. ISO 27001, an international standard for information security management, emphasizes risk management, incident response, and continuous monitoring—practices that could have minimized the impact of the attack on Indodax. COBIT, with its focus on governance and IT management, can help align security measures with broader business objectives, ensuring a proactive defense mechanism against such breaches.

A key part of implementing these frameworks involves conducting thorough system audits, regular employee training (to reduce phishing risks), and deploying advanced security controls. In Indodax's case, stronger monitoring of withdrawal systems and better authentication protocols might have thwarted the unauthorized transactions.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312001 |

As part of improving its defenses, Indodax and similar organizations should run regular security tests, including penetration testing and red-teaming exercises, to identify weaknesses. Simulated phishing attacks can also be used to assess how well internal staff respond to such threats, highlighting areas for further employee education and process enhancement. By continuously testing and refining these security measures, companies can stay ahead of evolving threats and reduce their vulnerability to future breaches.
Incorporating blockchain analytics tools to detect anomalous transactions early on can also help in proactively identifying security risks.

IV.COBIT and ISO 27001 INTEGRATION

To bolster cybersecurity defenses and mitigate vulnerabilities such as phishing attacks, organizations increasingly rely on structured frameworks like COBIT and ISO/IEC 27001. These frameworks provide comprehensive guidance for managing information security risks, ensuring compliance, and establishing robust internal controls. When integrated, COBIT and ISO 27001 offer a more holistic approach to risk management, combining governance, risk management, and operational security measures. Their integration also provides a strong defense mechanism against phishing attacks, which typically exploit weaknesses in an organization's people, processes, and technology.

4.1 COBIT (Control Objectives for Information and Related Technologies)

COBIT is an IT governance framework designed to help organizations develop, implement, monitor, and improve IT management practices. It provides a systematic approach to managing IT-related risks, ensuring that organizations align their IT goals with overall business objectives. COBIT addresses five key areas of governance: value delivery, risk management, resource management, performance measurement, and strategic alignment.
When it comes to cybersecurity, COBIT emphasizes risk management and control objectives that directly mitigate risks posed by phishing and other social engineering attacks. For instance, COBIT 2019 includes objectives for risk identification, IT asset management, incident management, and compliance, all of which can be leveraged to mitigate vulnerabilities caused by phishing attacks on internal staff. By adhering to COBIT's risk governance practices, organizations can improve their oversight of cybersecurity risks, establish accountability, and ensure that phishing-related risks are continuously monitored and addressed.

4.2 ISO/IEC 27001: Information Security Management Systems (ISMS)

ISO/IEC 27001 is a globally recognized standard for managing information security risks. The standard provides organizations with a framework to establish, implement, maintain, and continually improve an Information Security Management System (ISMS). ISO 27001 focuses on safeguarding the confidentiality, integrity, and availability of information by identifying and addressing security risks in a structured way.
The ISO 27001 framework involves a risk assessment process that helps organizations identify vulnerabilities—such as those introduced by phishing attacks—analyze their potential impact, and prioritize mitigation efforts. By aligning security controls with the standard's guidelines, organizations can implement effective defenses, such as advanced email filtering, incident response planning, and employee awareness programs. These practices, when designed under the ISO 27001 framework, not only reduce the risk of phishing but also ensure ongoing improvement through periodic audits and reviews of the security management system.

4.3 Integrating COBIT and ISO 27001 for Phishing Defense

By integrating COBIT's IT governance capabilities with ISO 27001's risk management focus, organizations can establish a comprehensive strategy for addressing phishing threats. The combined use of these frameworks enables organizations to manage security holistically, encompassing both governance and technical aspects of phishing defense.

4.4 Risk Identification and Management

COBIT and ISO 27001 both prioritize proactive risk identification and management, which are essential to mitigating phishing risks. The frameworks encourage organizations to conduct thorough risk assessments to understand where phishing vulnerabilities lie, such as weaknesses in employee awareness or email security systems. COBIT's governance structure ensures that the risk management process is aligned with overall business goals, while ISO 27001 provides specific guidelines for assessing and mitigating risks tied to phishing and social engineering attacks.
Through regular risk assessments, organizations can identify high-risk areas, such as employees with privileged access or departments handling sensitive data, and prioritize efforts to secure these vulnerabilities. This approach also enables organizations to continuously monitor evolving phishing tactics and ensure that controls remain effective against new threats.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312001 |

4.5 Enhanced Control Mechanisms

The integration of COBIT's control objectives with ISO 27001's security controls provides organizations with a solid foundation for developing, implementing, and enforcing security measures designed to defend against phishing attacks. COBIT's governance and management objectives, such as APO12 (Risk Management) and DSS05 (Manage Security Services), align with ISO 27001's Annex A controls, such as A.7.2 (Information Security Awareness, Education, and Training) and A.9.2 (User Access Management). These alignments ensure that security controls are not only technically sound but also strategically governed.

For example, ISO 27001's focus on employee training and awareness is directly supported by COBIT's emphasis on process governance and compliance. By integrating these, organizations can ensure that employees are not only trained to recognize phishing attacks but are also held accountable for adhering to security protocols and reporting potential threats. Additionally, ISO 27001's user access management controls, when aligned with COBIT's management objectives, ensure that access to critical systems is strictly monitored and controlled, reducing the risk of compromised credentials resulting from phishing.

4.6 Incident Response and Recovery

Another critical aspect of phishing defense is establishing effective incident response and recovery mechanisms. Both COBIT and ISO 27001 emphasize the need for well-structured incident management processes. ISO 27001 provides specific guidance on developing an incident response plan (Annex A.16), while COBIT's DSS02 (Manage Service Requests and Incidents) supports the creation of incident management workflows that are governed and consistently applied across the organization.

By combining COBIT's governance focus with ISO 27001's technical controls, organizations can ensure that their incident response capabilities are robust, efficient, and scalable. This integration is particularly useful for addressing phishing attacks, as it allows for rapid containment, forensic investigation, and recovery from compromised systems. Post-incident reviews and audits, as advocated by both frameworks, provide insights into the effectiveness of the response and help in refining future defenses.

4.7 Continuous Improvement and Monitoring

COBIT's emphasis on performance measurement (MEA01: Monitor, Evaluate, and Assess Performance) complements ISO 27001's requirement for continuous improvement (Clause 10: Improvement). Together, these frameworks encourage organizations to regularly review their cybersecurity policies, phishing defenses, and risk management processes to ensure they remain aligned with emerging threats. Organizations can implement key performance indicators (KPIs) to monitor the effectiveness of phishing prevention measures, assess employee awareness, and evaluate the overall maturity of their security posture.

For example, phishing simulation exercises and incident metrics can be used to evaluate the performance of email filtering systems, employee training programs, and incident response teams. These metrics help organizations identify areas that require improvement and ensure that both the governance structures (COBIT) and the technical controls (ISO 27001) are continuously enhanced to address new phishing tactics.

V.CONCLUSION

The integration of COBIT and ISO 27001 offers a powerful approach to managing cybersecurity risks, including those posed by phishing attacks targeting internal staff. By aligning COBIT's governance focus with ISO 27001's technical controls, organizations can create a comprehensive defense strategy that mitigates vulnerabilities, strengthens risk management practices, and ensures continuous improvement in security posture. With phishing attacks evolving in sophistication, the combined use of these frameworks provides organizations with the agility and resilience needed to prevent, detect, and respond to phishing threats effectively. Furthermore, by promoting strong governance, employee awareness, and technical controls, COBIT and ISO 27001 ensure that organizations are well-equipped to defend against future phishing attacks and other cyber threats.

REFERENCES

[1] Alshaikh, M. (2020). *Developing cybersecurity culture to influence employee behavior: A practice perspective.* Computers & Security, 98, 102003.

[2] Calder, A. (2016). *Implementing Information Security based on ISO 27001/ISO 27002: A Management Guide.* IT Governance Publishing.

[3] ISACA. (2019). *COBIT 2019 Framework: Introduction and Methodology.* ISACA.

[4] Jensen, M. L., Dinev, T., & Wright, R. T. (2017). *Phishing and human vulnerability: Exploring the susceptibility of humans to phishing attacks.* Journal of Information Privacy and Security, 13(3), 155-178.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312001 |

[5] Nohlberg, M., & Bäckström, G. (2017). *Phishing – Understanding and Mitigating the Human Factor in Cybersecurity.* International Journal of Cyber-Security and Digital Forensics, 6(1), 45-51.

[6] Blockhead. (2024). "Indonesian Crypto Exchange Indodax Suffers $22M Hack". https://www.blockhead.co/2024/09/12/indonesian-crypto-exchange-indodax-suffers-22m-hack/, accessed on 16 October 2024.

[7] Damimola, Lawrence. (2024). "Indodax Hacked for Over $22M as Security Breach Hits Hot Wallets". https://news.shib.io/2024/09/11/indodax-hacked-for-over-22m-as-security-breach-hits-hot-wallets/, accessed on 16 October 2024.

Cybersecurity Threats through Phishing Attacks Targeting Internal Staff, Mitigation and Prevention

ORIGINALITY REPORT

12%	11%	7%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Oklahoma Student Paper	5%
2	Aditya Nandan Prasad. "Introduction to Data Governance for Machine Learning Systems", Springer Science and Business Media LLC, 2024 Publication	2%
3	Dr. Jason Edwards. "Critical Security Controls for Effective Cyber Defense", Springer Science and Business Media LLC, 2024 Publication	1%
4	www.coursehero.com Internet Source	1%
5	www.ijareeie.com Internet Source	1%
6	www.ispartnersllc.com Internet Source	1%
7	Submitted to American Intercontinental University Online	1%

Student Paper

8	fastercapital.com Internet Source	1 %
9	Submitted to United Colleges Group - UCG Student Paper	1 %
10	www.island.io Internet Source	1 %

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		