International Journal of Computer Engineering and Technology (IJCET)
Volume 13, Issue 1, January-April 2022, pp. 87-97, Article ID: IJCET_13_01_008
Available online at https://iaeme.com/Home/issue/IJCET?Volume=13&Issue=1
ISSN Print: 0976-6367 and ISSN Online: 0976–6375
Impact Factor (2022): 17.98 (Based on Google Scholar Citation)
DOI: https://doi.org/10.34218/IJCET_13_01_008

PHISHING SIMULATION AUTOMATION: GOPHISH CAMPAIGNS WITH AZURE AD CONDITIONAL ACCESS AND USERRISK-BASED TRAINING

Sandhya Guduru,
Masters in Information Systems Security,
Software Engineer - Technical Lead, USA.

ABSTRACT

Phishing remains one of the most persistent threats to organizational cybersecurity. This study presents an automated framework integrating Gophish-based phishing simulations with Microsoft Azure Active Directory (Azure AD) to enhance user awareness and response. The system leverages Azure AD's UserRisk scores to identify high-risk individuals and dynamically applies Conditional Access policies to restrict access following a phishing attempt. Upon detecting risky behavior, affected users are enrolled in SCORM-compliant cybersecurity training tailored to their actions. PyTorch-based Natural Language Processing (NLP) models analyze click-through behavior, enabling adaptive content delivery. This research demonstrates a closed-loop mechanism that detects, responds to, and educates users quickly, reducing organizational vulnerability to social engineering attacks.

Keywords: Phishing simulation, Gophish, Azure AD, Conditional Access, UserRisk, SCORM training, cybersecurity automation, NLP, PyTorch, phishing awareness, user behavior analysis.

Cite this Article: Sandhya Guduru. (2022). Phishing Simulation Automation: Gophish Campaigns with Azure AD Conditional Access and UserRisk-based Training. *International Journal of Computer Engineering and Technology (IJCET)*, 13(1), 87-97. https://iaeme.com/Home/issue/IJCET?Volume=13&Issue=1

1. Introduction

Phishing attacks pose a significant threat to organizational cybersecurity and account for many data breaches and security incidents worldwide. Despite ongoing efforts in security awareness training, many users remain vulnerable to socially engineered emails, resulting in compromised credentials, unauthorized access, and financial loss. Traditional phishing prevention strategies, such as static training modules and blanket email filters, lack the adaptability and real-time response to counter evolving attack vectors and user behaviors [1] [2].

In response to this challenge, there is a pressing need for dynamic, data-driven approaches that personalize user training and enforce security policies based on individual risk profiles. This research introduces an automated phishing simulation and response framework integrating Gophish with Microsoft Azure Active Directory (Azure AD) UserRisk scoring and Conditional Access policies. The proposed system continuously monitors user interactions with phishing simulations and adjusts access permissions accordingly, ensuring that high-risk users are promptly contained].

To complement this, the framework incorporates SCORM-based cybersecurity training modules automatically assigned based on user performance in phishing tests. Furthermore, by leveraging PyTorch-based Natural Language Processing (NLP), the system analyzes user click-through behavior to generate personalized training content, enhancing its relevance and effectiveness.

This paper explores the integrated framework's architecture, implementation, and impact in reducing user susceptibility to phishing and improving organizational readiness. By uniting simulation, risk analytics, access enforcement, and adaptive training, the solution aims to bridge the gap between security policy enforcement and end-user behavior modification].

2. Literature Review

Phishing attacks remain one of the most pervasive cybersecurity threats, with attackers continuously evolving their strategies to exploit human behavior. In response, organizations have begun adopting more sophisticated approaches that combine phishing simulations, identity protection mechanisms, and personalized training. Integrating these technologies offers the potential for more effective security awareness programs and a more secure enterprise environment. This literature review explores key developments in phishing simulation, identity protection with Azure AD, and personalized training through SCORM-based modules and Natural Language Processing (NLP).

2.1. Phishing Simulations and User Behavior Analysis

Phishing simulations have become a cornerstone of modern cybersecurity awareness programs [1]. Tools such as Gophish simulate phishing attacks by sending deceptive emails to employees and tracking their responses, including clicking links, downloading attachments, or entering sensitive information. The effectiveness of these simulations is well-documented, as they help to increase employee awareness and reduce susceptibility to real attacks [3]. However, many phishing simulation tools are limited by their generic nature, offering a one-size-fits-all approach that does not consider the varying risk levels among users. As a result, users frequently targeted by phishing attempts or exhibiting risky behavior often continue to fall for these attacks, and the overall effectiveness of the simulation diminishes over time[4].

Some recent studies have highlighted the importance of personalized phishing simulations tailored to individual user behaviors. However, existing platforms often fail to adjust the difficulty or content of simulations based on a user's past performance. This creates a gap in effectiveness, particularly for high-risk individuals who may need more intensive training or focused interventions [4].

2.2. Risk-Based Access Control with Azure AD

Azure Active Directory (AD) provides advanced identity and access management features, including UserRisk scores and Conditional Access policies. Azure AD's risk-based approach evaluates user behaviors such as login location, device security posture, and sign-in anomalies to assign a risk score [5]. Based on the assessed risk, this score can trigger conditional access policies to limit access to sensitive resources. While these features significantly enhance security by dynamically adapting to user behaviors, limited research has been done on integrating phishing simulations directly with these risk-based policies.

By combining phishing simulations with Azure AD's UserRisk scores, organizations could automatically apply stricter access policies to users who fail simulations or exhibit high-risk behavior. This integration would enable a more responsive and adaptive security environment, addressing risky behaviors in real-time and reducing the likelihood of successful attacks. The literature suggests that combining both elements—phishing simulations and identity risk scoring—could lead to a more robust, proactive cybersecurity strategy, yet this remains an underexplored area in existing research [5].

2.3. Personalized Cybersecurity Training with SCORM and NLP

Traditional cybersecurity training programs are often static, relying on standardized content delivered via Learning Management Systems (LMS) using the SCORM (Sharable Content Object Reference Model) standard. While SCORM provides an efficient framework for delivering and tracking training modules, the lack of personalization limits its effectiveness. Users who struggle with certain topics or need more focused guidance may find the training irrelevant, undermining the overall learning experience [6].

Incorporating Natural Language Processing (NLP) into training platforms offers a promising solution. By analyzing user interactions with training materials and phishing simulations, NLP algorithms can dynamically adjust the content to better suit the user's learning needs [7]. For instance, if a user repeatedly clicks on phishing links, the system could generate more tailored training modules to address specific weaknesses, improving retention and engagement. Research has shown that personalized training is far more effective in reinforcing cybersecurity concepts and mitigating human error [7]. Despite the promise of NLP-based training, very few studies have integrated it with phishing simulations or identity management systems, leaving a gap in its application for cybersecurity training.

2.4. Challenges and Research Gaps

While the individual components of phishing simulations, risk-based access controls, and personalized training have been studied extensively, integrating these technologies into a unified workflow remains a significant challenge. Organizations often implement these systems independently, leading to inefficiencies and delayed responses to high-risk behaviors. An essential limitation of existing research is the lack of automated systems that connect phishing simulation outcomes with identity risk scores and enforce relevant access controls or trigger personalized training [3].

Furthermore, despite the significant potential of integrating PyTorch NLP models to personalize training content, the existing literature lacks detailed frameworks that connect

machine learning-based content tailoring with phishing simulation results [8]. Without a cohesive system that links all these elements—phishing simulations, real-time risk scoring, dynamic access control, and personalized training—organizations are left with fragmented security awareness programs that fail to provide real-time feedback and adjustments based on evolving user behavior.

2.5. Integration of Phishing Simulations and User Risk Scoring

One of the most pressing issues in cybersecurity today is the disconnect between phishing simulations and user behavior analytics. Integrating simulation results with identity protection tools like Azure AD's Conditional Access policies could provide a more holistic approach to securing an organization. Organizations can enforce a more proactive defense mechanism by automatically adjusting access control based on the outcomes of phishing simulations (such as blocking access to critical systems for users who fail simulations).

Despite this potential, research on such integrated solutions remains sparse. Existing studies focus mainly on phishing simulations or identity management separately, with little attention given to the benefits of combining these two elements. Furthermore, most approaches cannot continuously monitor and update risk scores in real time based on user interactions with training materials, creating a reactive rather than proactive approach to mitigating phishing threats.

3. Problem Statement: Challenges in Phishing Simulation Automation with Azure AD UserRisk and Gophish Campaigns

Phishing attacks are one of the most prevalent and damaging forms of cybercrime. They target organizations through deceptive emails and other communication methods designed to steal sensitive information. Despite technological advancements in firewalls, anti-malware software, and email security filters, phishing attacks remain effective because they exploit the human element—the weakest link in an organization's cybersecurity defenses. Employees continue to fall victim to well-crafted phishing emails, leading to breaches, financial losses, and reputational damage.

While many organizations have implemented phishing simulation campaigns as a proactive training measure, these initiatives are often inconsistent, ineffective, or insufficient in reducing the risk of phishing-related breaches. Current phishing simulation tools like Gophish provide valuable testing environments to educate users, but they typically operate in a generalized manner. In many cases, the simulations are conducted without considering an

individual's risk level, meaning all employees are exposed to the same threat level regardless of their specific behavior patterns or susceptibility to phishing.

Moreover, traditional phishing simulations do not integrate real-time data about user behavior, making it difficult to adjust the training experience based on how users respond to phishing attempts. As a result, employees who may have fallen victim to phishing campaigns in the past or are classified as high-risk by security tools are treated the same as users with minimal risk exposure. This one-size-fits-all approach limits the effectiveness of training programs because it fails to tailor content to the needs of individual users.

Integrating Azure Active Directory (Azure AD), the UserRisk score offers a more personalized and data-driven approach to phishing simulation. These scores are generated based on a user's historical behavior, login activity, and other risk factors within the organization's environment. However, many organizations fail to link UserRisk scores to phishing campaigns, missing an opportunity to target employees at the highest risk of being tricked by phishing attacks. Without this connection, the simulations are not as effective, and organizations cannot focus their efforts on the most vulnerable users.

In addition, Azure AD Conditional Access policies, which control access to corporate resources based on a user's risk level, are not often connected to phishing simulation platforms. Conditional Access policies are essential to modern cybersecurity, as they enforce stricter access controls for users who show higher-risk behaviors. However, when phishing simulations are conducted independently of these policies, they fail to implement the "least privilege" principle and risk-based access control. This creates a disconnect between the organization's security posture and its employee training efforts.

Another challenge lies in the training component of phishing simulations. While SCORM-based training provides a practical framework for delivering online educational content, it cannot dynamically adjust based on a user's specific interaction with phishing campaigns. Most SCORM-compliant systems deliver static content and fail to integrate with phishing simulation tools in a way that can provide personalized feedback or tailor content based on real-time behavior. This limits the potential for users to receive targeted educational content that addresses their specific vulnerabilities, reducing the overall impact of the training.

As phishing simulation tools, user risk scores, and training systems operate in silos within many organizations, the ability to provide a comprehensive, data-driven solution for preventing phishing attacks is hindered. This leads to operational inefficiencies, reduced effectiveness of training programs, and an overall increase in vulnerability to phishing attacks.

To address these challenges, a comprehensive solution that integrates Gophish phishing simulations, Azure AD UserRisk scores, Conditional Access policies, and SCORM-based training is required. Such a solution would automate phishing campaigns dynamically tailored to individual users' risk profiles, ensuring that high-risk users are subjected to more rigorous testing and personalized training. Moreover, the system should integrate PyTorch-based NLP (Natural Language Processing) techniques to analyze user click-through behavior and further refine the content of the phishing simulations. This would enhance the precision of simulations and help create personalized training modules that evolve with user behavior, providing a tailored learning experience.

Additionally, integrating these components would allow organizations to enforce real-time access controls and provide mandatory, risk-based training for all users. This would help to bridge the gap between phishing simulations, access control policies, and employee training programs, ultimately improving an organization’s resilience to phishing threats and enhancing overall cybersecurity hygiene.

4. Proposed Solution

To address the challenges of phishing attacks and ensure a robust defense strategy, the proposed solution automates phishing simulation campaigns by integrating Gophish with Azure Active Directory (Azure AD) UserRisk scores. This integration allows organizations to tailor phishing simulations and security training programs based on user-specific risk profiles, ensuring that high-risk individuals receive targeted education and that security policies are enforced efficiently.

The first key element of the solution is Gophish phishing simulations. Gophish, an open-source phishing simulation tool, allows organizations to design realistic and customizable phishing campaigns. These campaigns simulate common phishing tactics such as deceptive emails, fake login pages, and social engineering strategies. By linking these campaigns to Azure AD UserRisk scores, the system can dynamically adjust the level of simulation based on the user’s risk profile. For example, users flagged with higher risk scores (such as those exhibiting suspicious login patterns or other risky behavior) will receive more challenging and targeted phishing attacks. This ensures that users more likely to fall victim to attacks are given more focused training and intervention.

The second component of the solution is Azure AD UserRisk scores, which measure the likelihood that a given user will be targeted or fall for a phishing attack. Azure AD analyzes

user activity (e.g., failed login attempts, unfamiliar location logins) to assign a risk score, indicating whether the user is more likely to be compromised. This score then prioritizes users for phishing simulations and customizes their security training. By incorporating UserRisk into the simulation process, the solution can automatically adjust the phishing simulations' frequency, difficulty, and content based on the user's individual risk level. This targeted approach increases the likelihood that the training will resonate with users and that they will become more aware of phishing threats.

Conditional access policies are another essential feature of the solution. By leveraging Azure AD's conditional access framework, the solution can enforce stricter security controls for high-risk users identified by the UserRisk score. These controls may include requiring multi-factor authentication (MFA), restricting access to certain resources, or limiting access from specific locations or devices. Such policies add an extra layer of protection for users who have been identified as high-risk, ensuring that even if they fall victim to a phishing attempt, the potential damage is minimized. This proactive approach to risk management helps ensure that the organization’s security posture remains strong.

A vital part of the solution is SCORM-based mandatory training. SCORM (Sharable Content Object Reference Model) is a widely used standard for eLearning content. By delivering training content through SCORM, organizations can ensure that users complete mandatory training sessions tailored to their behavior. The content is dynamically adjusted based on user interaction with phishing simulations and click-through behaviors. For example, if a user clicks on a simulated phishing link during a campaign, they will be automatically redirected to a training module focused on identifying phishing attempts. This personalized training approach maximizes the effectiveness of each session and ensures that employees are better equipped to recognize and avoid phishing scams in the future.

Lastly, PyTorch NLP behavior analysis is crucial in further personalizing training content. Using Natural Language Processing (NLP) techniques in PyTorch, the system can analyze user interaction patterns with phishing emails. NLP allows for identifying language cues, patterns, and behaviors that indicate a user's vulnerability or tendency to fall for specific phishing attacks. This analysis helps tailor the training content to address the specific weaknesses of each user, offering personalized guidance on how to spot and avoid phishing tactics. This approach ensures that the training is not one-size-fits-all but adapted to individual users' unique behaviors, leading to more effective learning outcomes.

In combination, these components form a comprehensive solution that automatically detects and responds to user vulnerabilities, personalizes training efforts, and enforces security measures in real-time. The result is a system that not only educates employees about phishing but also integrates security measures directly into their workflow, making it easier for organizations to maintain a high level of security without requiring constant manual intervention. The solution offers a dynamic and proactive approach to phishing prevention by continuously monitoring user risk and adapting to changing behaviors.

This method improves security awareness, reduces susceptibility to phishing attacks, and ultimately leads to a more secure organization overall.

Component	Description	Benefits
Gophish Simulations	Phishing campaigns linked to Azure AD UserRisk scores.	Targets high-risk users effectively.
Azure AD UserRisk	Scores indicating phishing risk based on behavior.	Focuses on at-risk users for intervention.
Conditional Access	Policies like MFA triggered by UserRisk scores.	Enhances security for risky users.
SCORM-based Training	Mandatory, personalized training based on user behavior	Improves training effectiveness.
PyTorch NLP	Adjusts content based on user click-through behavior.	Customizes training to user weaknesses.

This table captures the key elements of the solution, their descriptions, and the benefits they provide in creating a comprehensive, automated phishing simulation and training system.

5. Conclusion

In conclusion, integrating Gophish campaigns with Azure AD Conditional Access and UserRisk-based training provides a robust, automated solution for enhancing organizational cybersecurity. By leveraging Gophish's capabilities to simulate phishing attacks and Azure AD's real-time risk assessments, this approach offers a dynamic, targeted method for identifying user vulnerabilities. Conditional Access policies and UserRisk scores enable the tailoring of security training, ensuring that most at-risk users receive immediate and personalized interventions. This automation not only streamlines the phishing simulation process but also ensures that training is relevant and responsive to the individual risk profiles

of users. As cybersecurity threats evolve, adopting such adaptive and automated solutions will foster a culture of continuous learning and resilience against phishing attacks. Future work in this area could explore further automation techniques, including integration with additional threat intelligence tools and advanced machine learning models, to continually enhance the effectiveness of phishing simulation and training programs.

References

[1] I. Qabajeh, F. Thabtah, and F. Chiclana, "A recent review of conventional vs. automated cybersecurity anti-phishing techniques," Computer Science Review, vol. 29, pp. 44–55, Aug. 2018, doi: https://doi.org/10.1016/j.cosrev.2018.05.003.

[2] Hossain Shahriar and M. Zulkernine, "PhishTester: Automatic Testing of Phishing Attacks," Jan. 2010, doi: https://doi.org/10.1109/ssiri.2010.17.

[3] E. Blancaflor et al., "Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools," 2021. Available: https://ieomsociety.org/singapore2021/papers/1105.pdf

[4] Y. Li, K. Xiong, and X. Li, "An Analysis of User Behaviors in Phishing eMail using Machine Learning Techniques," 2019. https://behavior.isi.jhu.edu/publications/SECRYPT_2019_95_CR[4440].pdf

[5] H. Jauhiainen, "Designing End User Area Cybersecu- rity for Cloud-based Organization," 2021. Available: https://www.theseus.fi/bitstream/handle/10024/467445/Designing%20End%20User%20Area%20Cybersecurity%20for%20Cloud-based%20Organization.pdf?sequence=2

[6] T. Tang and Dat, "Automatic Cyberattack Emulation for Interactive Security Defense Training," 2017. Available: https://dspace.jaist.ac.jp/dspace/bitstream/10119/14797/5/paper.pdf

[7] M. Taeb and H. Chi, "A Personalized Learning Framework for Software Vulnerability Detection and Education," 2021. https://www.researchgate.net/profile/Maryam-Taeb/publication/357291103_A_Personalized_Learning_Framework_for_Software_Vulnerability_Detection_and_Education/links/62e157139d410c5ff36924f9/A-

Personalized-Learning-Framework-for-Software-Vulnerability-Detection-and-Education.pdf

[8] D. Rao and B. McMahan, “Natural Language Processing with PyTorch,” Google Books, 2019. https://books.google.com.pk/books?hl=en&lr=&id=Gh-EDwAAQBAJ&oi=fnd&pg=PP1&dq=++PyTorch+NLP+models&ots=xvWc5CiSmA&sig=K3zNS9IuzfiIWwVkUYR9PDhNA10&redir_esc=y#v=onepage&q=PyTorch%20NLP%20models&f=false