IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46ICT/2025/4635525/
Vol. 2025 (35), Article ID 4635525

Identity Protection in Managing Access to Public Cloud Services: Lessons from Phishing Simulation Tests*

Piotr ZDUNEK

Faculty of Cybernetics, Military University of Technology, 2 Kaliskiego st. 00-908 Warsaw, Poland,

Correspondence should be addressed to: Piotr ZDUNEK, piotr.zdunek@student.wat.edu.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

Digital identities have become an integral component of using online services in both personal and professional contexts. They constitute the primary mechanism for authenticating access to cloud computing services, where confidential information is often processed. Unauthorized access to such data can result in severe financial, operational, and reputational consequences, making digital identities one of the main targets for cybercriminals. The increasing number of incidents involving compromised identities highlights the need to adopt more effective protection methods. Despite the growing number of publications on cybersecurity, existing research offers limited examination of the relationship between the effectiveness of phishing attacks and the protection of digital identities in public cloud services. As part of this study, a series of controlled phishing simulations were conducted across several organizations operating in different sectors, involving a total of 3,891 users. The phishing emails were designed to closely resemble real-world campaigns used by cybercriminals to target cloud services, and the collected data included message open rates, clicks on malicious links, and instances of credential disclosure, which were subsequently subjected to detailed quantitative analysis. The results revealed significant differences in user behaviour depending on the nature of the organizations' operations. These findings clearly indicate the need to further strengthen digital identity protection, as users exposed to various social engineering techniques tend to disclose their authentication credentials. Consequently, this paper presents a set of recommendations and methods for securing identities and managing access in cloud computing environments, ultimately contributing to the development of a comprehensive identity security model.

Keywords: digital identity security, cybersecurity, identity and access management (IAM), cloud computing security

Introduction

In 2023, 45.2% of companies in the EU purchased cloud computing services for hosting their e-mail systems, storing files in electronic form and using office software (Eurostat, 2023). In Poland alone, compared to 2021, the use of cloud services by enterprises increased by 27 percentage points reaching 53%, including as many as 88.4% of large companies employing more than 250 people (Gumiński et al., 2023). This trend is naturally consequence of dynamic development of digital technologies and e-services. Rapid and easy access to entire platforms enabling companies to initiate IT-driven business processes with minimal delay is one of the biggest advantages of cloud computing. Moreover, enterprises can provide their electronic services worldwide with minimal network latency regardless of where the users are located. The same applies to employees working remotely. According to the Eurostat (2025), 22.2% of people aged 15 to 64 usually or occasionally work from home. Both remote and on-site employees use their account to login in to cloud environment, software and systems where companies' resources are processed. They gain access to email and office software to create, store and share documents and files, as well as to communicate online. Although, this approach improves work efficiency and flexibility, it also exposes enterprises to additional risks. Systems and data stored and processed in cloud environments have become a valuable target for cybercriminals. The rise of cyber threats such as hacking, data breaches, phishing and ransomware has highlighted the need for robust security measures to protect cloud computing infrastructure and

Cite this Article as: Piotr ZDUNEK, Vol. 2025 (35) "Identity Protection in Managing Access to Public Cloud Services: Lessons from Phishing Simulation Tests " Communications of International Proceedings, Vol. 2025 (35), Article ID 4635525, https://doi.org/10.5171/2025.4635525

cloud data (Liang and Xu, 2025). Once compromised, systems are frequently exploited as footholds for lateral movement and as platforms (e.g., botnets, phishing platform) to execute further attacks. Stolen or encrypted data may be used to blackmail victims, often by leaking the stolen information on the Internet. In addition, ransomware incidents can cause severe disruptions to business continuity and operational processes.

Many resources, software and configuration types deployed in public cloud services often leads organizations to overlook the consequences of incidents caused by incomplete security polices, configuration errors, and a lack of appropriate access management and monitoring procedures. Information processed in the cloud often contains trade secrets or sensitive data. Unauthorized access may result in a range of serious losses, such as:

- Financial losses – direct costs resulting from the theft of a company's intellectual property, financial penalties for violations of laws and regulations, and expanses related to incident response.
- Reputational damage – loss of trust among customers, business partners, and investors.
- Loss of competitive advantage – theft of trade secrets, business strategies, or intellectual property, including innovative solutions or products before their market release.
- Operational disruption – interruptions or loss of access to company services and products.
- Legal and regulatory consequences – liabilities arising from non-compliance with applicable laws or industry regulations.
- Threats to personal security – breaches of privacy affecting customers, employees or business partners.

The paper describes the fundamental elements of public cloud security, with particular emphasis on identity and access management. The phishing tests conducted in several organizations support the author's observation that proper identity protection and access rights management constitute one of the key pillars of cloud security. Proper configuration and implementation of security measures allow for effective mitigation of risks associated with cyberattacks and the previously described losses. Section 2 presents the fundamental principles of ensuring security in public cloud. Section 3 describes the phishing simulation tests conducted within selected organizations and discusses their results. Section 4 provides a detailed overview of identity and access management principles. Finally, Section 5 presents the conclusions.

Public Cloud Security

One of the fundamental principles of public cloud security is the shared responsibility model, which defines how security obligations are divided between the cloud provider and the customer. A proper understanding of this model is essential, as it determines which components of the cloud environment administrators are responsible for securing. Misinterpretation of the shared responsibility model may result in security oversights and, consequently, successful cyberattacks on the infrastructure. According to the Google Cloud (2023), responsibility allocation varies depending on the selected cloud service delivery model, which includes the following types:

- IaaS (Infrastructure as a Service) – cloud provider delivers on-demand infrastructure to organizations, such as compute, storage, networking and virtualization.
- PaaS (Platform as a Service) – cloud provider delivers and manages all the hardware and software resources to develop applications through the cloud. Customer is not required to manage and maintain environment to build and deploy applications.
- SaaS (Software as a Service) – cloud provider provides the entire application stack, delivering an entire cloud-based application that customers can access and use. Most SaaS applications are accessed directly through a web browser.

Simplifying the approach to cloud security responsibility, two terms can be adopted: "*security of the cloud"* and "*security in the cloud"*. Term "*security of the cloud"* applies only to cloud provider, who delivers and ensures physical security of data centres and cloud infrastructure components, such as physical network devices and connections, servers, and data storage arrays. Providers use the latest security measures, such as surveillance cameras, imposing tools to control access to data and services, biometric authentication, physical security barriers and other methods that ensure the physical security of the infrastructure and servers (Al-Qtiemat and Al-Odat, 2024). On the other hand, the term *"security in the cloud"* refers to the shared responsibility between the cloud provider and the customer, depending on the chosen cloud service delivery model. The customer is responsible for the resources they launch in the cloud, while the provider is responsible for the underlying infrastructure required to host them. It is important to note that the customer is always responsible for information and data, regardless of whether this data is processed, transmitted or stored using any resource available in the cloud. The same applies to identities and accounts, as customers are responsible for controlling who can access their public cloud resources and with what permissions.

Preserving data and applications in the cloud is extremely important. Therefore, the implementation of security measures must be ensured by applying the necessary security strategies (Al-Qtiemat and Al-Odat, 2024). Cloud providers offer a range of tools and mechanisms that enable the implementation of multi-layered protection, effectively minimizing the risk of breaches to the confidentiality, integrity, and availability of processed data and the cloud environment. When developing a security strategy, it is important to properly classify data, resources and applications according to their business value. Furthermore, it is important that all elements that make up the cloud environment are secured in an automated and continuous manner to ensure constant control, which will reduce the risk of human error and system vulnerabilities.

Enterprises aiming to ensure comprehensive cloud security should consider the fundamental security domains that, according to the author, are mutually complementary and together create a consistent security model in the cloud. This model includes the following domains:

- Identity security and access management,
- Network security,
- Data storage and database security,
- Application and cloud resource security,
- Monitoring and Logging,
- Continuous configuration improvement,
- Compliance and regulations.

Each of these strategies requires the implementation of specific mechanisms and controls to ensure their full effectiveness.

Phishing Simulation Tests

As part of the study, a series of phishing campaigns was carried out across 10 enterprises representing various industries, including finance, public administration, construction, manufacturing, IT services, and logistics. In total, phishing emails were sent to 3981 users. The main element of the phishing campaign was a fake email informing the user that their cloud storage space was full. To increase the available storage, the user had to click the “Expand disk” button. After clicking the button, the user was redirected via a malicious link to a phishing website that requested authentication credentials (login and password). Once the credentials were entered, the page redirected the user to the legitimate website of one of the public cloud providers with office applications. Both email and suspicious web page impersonated actual office services in public cloud used by companies. Each user action, reading the email, clicking the link, and entering authentication credentials was tracked and recorded for statistical analysis. These data are presented in Table 1.

Table 1: Summary of Phishing Simulation Test Results

Industries	Email Sent	Email Opened	Clicked Link	Submitted authentication data
Manufacturing	980	250	115	57
IT services	470	289	57	20
Finance	195	32	12	4
Construction	1479	678	438	310
Public administration	109	49	44	0
Logistics	658	154	124	22
Total	**3891**	**1452**	**790**	**413**

Table 2: Percentage Summary of User Actions During Phishing Simulation Tests

Industries	% of Emails Opened (of All Tested Users)	% of Link Clicks (of All Tested Users)	% of Submitted data (of All Tested Users)	% of Link Clicks (of Opened Emails)	% of Submitted data (of Opened Emails)
Manufacturing	25,51	11,73	5,82	46	22,8
IT services	61,49	12,13	4,26	19,72	6,92
Finance	16,41	6,15	2,05	37,5	12,5
Construction	45,84	29,61	20,96	64,6	45,72
Public administration	44,95	40,37	0	89,8	0
Logistics	23,4	18,84	3,34	80,52	14,29
Total	**37,32**	**20,3**	**10,61**	**54,41**	**28,44**

The results of the study (Table 2) show that 37.32% of all tested users opened the phishing email, and 10.61% of them entered their login and password on the phishing website. Furthermore, 54.41% of users who opened the suspicious email clicked the embedded link, and 28.44% of them entered their login credentials on the malicious website. The highest number of compromised users originated from the construction sector, while none were recorded in the public administration sector, even though the highest percentage of its users clicked the link. Simply clicking the link can also lead to a compromise, for example, through the exploitation of a web browser's vulnerability or by downloading an additional malicious attachment to the victim's computer.

Credential data obtained in this way can be used by cybercriminals to gain unauthorized access to cloud services and to exfiltrate sensitive information, such as emails, documents, images, photos, and other files. Access to such data may expose the organization to the serious consequences presented in the introduction. In addition, attackers may leverage the stolen credential to gain access to more types of resources, as virtual machines, applications, data bases or even entire public cloud infrastructure, when the comprised account has administrative privileges. These risk and other related issues must be prevented or mitigated. In summary, the results of this research show that identity security and proper access management are among the most important strategies for ensuring confidentiality, integrity and availability in public cloud environments. Therefore, the following sections of this article describe the fundamental principles of identity security and access management.

Identity Security and Access Management

Research conducted by Google Cloud (2024) based on information about incidents in their customers' environments, shows that 51% of cases of cloud instance compromise were due to weak or missing authentication credentials. The purpose of ensuring identity and access security in a cloud environment is to protect from unauthorized and improper use, which is a key element of cybersecurity strategy in modern IT ecosystems.

Cloud identities can be divided into two groups:

- User Identities – account dedicated specifically to individuals (workers, administrators) in the organization, users outside the organization (guests, suppliers), federated accounts (managed by other identity systems).
- Managed & Service Identities – identities intended for applications, services, resources, and systems that require appropriate permissions and access to perform their assigned tasks.

A conscious approach to security policy and the use of appropriate tools offered by public cloud computing enable effective access control and identity management by user provisioning and de-provisioning, ensure that only authorized users can access cloud resources, and maintain an extensive audit trail for monitoring and compliance purpose. Due to the dynamic nature of cloud environments, user rotation, and the frequent creation of test environments or new instances, organizations often encounter challenges in managing identities and access privileges effectively. Identities in the cloud tend to change over time, new user and service accounts are created, while others become outdated. In some cases, default access policies often persist after deployment, which can lead to weak authentication and overly broad authorization to cloud resources. As mentioned earlier, preventing identities from being compromised is extremely important, so the implementation of security measures must be ensured by applying the appropriate security principles.

Fundamental principles of identity and access protection include:

I. Zero Trust Model

The concept of Zero Trust is increasingly being discussed. It refers to a security approach that applies the principle of least trust to users, resources and assets (Rose et al., 2020). In this approach, all elements of the cloud environment should be considered untrusted until their access requests to specific parts of the environment have been verified. Furthermore, the Zero Trust model is based on the principle of *"never trust, always verify*", regardless of where the access request originates. Once the integrity of the requesting entity has been verified, access should be granted conditionally, according to the assigned level of trust, established security policies, and the sensitivity of the target resources. The trust validation process should rely on all available information points about the requesting entity, including its digital identity, geolocation, the security posture of devices or resources used to gain access, authentication methods, access context, and data sensitivity. In addition, every access authorization to data or infrastructure should be preceded by a thorough risk assessment related to the requested access.

II. Principle of Least Privilege (PoLP)

This principle is closely related to the Zero Trust model, which assumes that no user or device should be trusted by default, regardless of whether it is located inside or outside the organization. Every access request to resources must therefore be verified, monitored, and controlled. According to the PoLP, every entity, whether a user, process, application, or a device should have only the minimal permissions and access rights necessary to perform its assigned task. Moreover, this means that access to resources should be strictly limited and aligned with actual operational needs. Continuous review and adjustment of access rights are essential to maintaining compliance with this principle and minimizing the risk of privilege misuse.

III. Strong Authentication

Authentication is the process of confirming identity, during which an entity proves that it is who or what it claims to be (Łąka, 2024). Strong authentication process should be protected according to the following rules:

- Strong password policy – passwords or secrets used for authentication, in accordance with the best practices outlined by the National Institute of Standards and Technology (NIST), should contain at least 15 characters. Passwords should be checked against databases of known or previously compromised passwords to prevent their reuse. In addition, periodic password expiration (e.g., every 30 or 90 days) is not recommended (Temoshok et al., 2025), as it may lead to the creation of predictable and weaker passwords, increasing the risk of password reuse across multiple systems. Building strong user passwords does not rely on creating complicated, unmemorable strings. Instead, users can create strong and memorable passphrases while avoiding dictionary words. For example, the password "One2treeHideMayCat%" would be both strong and memorable, yet very difficult to crack. For passwords or secrets used by services and systems, the simplest and most secure approach is to generate them automatically and store them in dedicated password vaults or secret management systems.
- Multi-Factor Authentication (MFA) – MFA adds an additional layer of verification to the authentication process by combining different types of authentication methods (Suleski et al., 2023), such as:
    - Knowledge - "something you know" – a password or PIN known to the user.
    - Possession - "something you have" – a physical device, such as a hardware token, security key, code card, or mobile authentication application.
    - Inherence - "something you are" – typically biometric verification.

  Even if one of the authentication factors is compromised, multi-factor authentication still helps protect digital identities, provided that the user does not disclose the second factor, such as a token,

or approve a push notification for an unauthorized login on a mobile authentication application. Using a physical security key is a strong authentication method, as it must be connected to the client device attempting to log in. Therefore, a cybercriminal who has stolen a user's credentials and attempts to log in from another location using a different device would be unable to do so.

IV. Privileged Access Management

Special attention should be paid to privileged identities, which have significantly extended permissions and access to critical resources. Such accounts are often used to manage cloud infrastructure and its components. Unauthorized access to these accounts can have severe consequences for the security of the infrastructure, data, and the integrity of information processes. Frequently, these accounts become vectors for large-scale attacks. For example, the compromise of a domain administrator account may result in the distribution of ransomware within the organization's domain, leading to the encryption of data on servers and workstations.

In addition to the identity protection methods described earlier, accounts with high privileges should be secured using Privileged Access Management (PAM) and Privileged Identity Access Management (PIM) systems. According to Łąka (2024), such systems facilitate the control and oversight of privileged access. These systems serve the following purposes:

- Session management – allows administrators to terminate a session at any time if an account has been compromised or exhibits suspicious activity.
- Password management – enables the sharing of credentials with authorized users and allows passwords to be changed after each use or when necessary.
- Roles and groups – allow the assignment of appropriate roles and groups to privileged accounts, ensuring that such accounts have permissions and access rights in accordance with the PoLP.
- Access approval – enables the granting of specific access rights to an account in a controlled manner by a superior or authorized person. It is also possible to grant elevated privileges or temporary access for a strictly defined period (Just-in-Time), after which the account automatically loses these permissions.
- Monitoring – provides continuous monitoring of user activities and tasks performed within privileged sessions.

V. Federated Identity Management

In public cloud, external identity providers (e.g., Google, Microsoft) are often used for authentication. Through Single Sign-On (SSO) and identity federation, it is possible to use the same identity across multiple platforms and applications. Although this approach simplifies the authentication process, to ensure security, access to organizational resources should be granted only to users and applications explicitly authorized by the organization. Once properly authenticated, these accounts should be allowed to access only designated applications, data, and resources within the specific environment. Additionally, organizations should continuously monitor which external systems their users authenticate to and assess whether such access is appropriate.

VI. Monitoring

All activities related to account and resource access should be continuously monitored and audited for forensic purposes and compliance reasons. Monitoring identities and assigned privileges in public cloud environments must include real-time activity to detect and respond to potential threats. The detection of suspicious behaviour may involve the following:

- Unauthorized access attempts – monitoring systems can detect unauthorized authentication attempts of efforts to gain access to resources for which the user does not have the required permissions.
- User behaviour anomalies – artificial intelligence and machine learning techniques can be used to detect behavioural anomalies based on historical user activity. Examples include sudden activity during unusual hours, access from unfamiliar locations, or attempts to perform operations on many resources within a short period of time.
- Privilege modification – monitoring activities related to the assignment and modification of user permissions may help identify cases where excessive privileges are granted or attempts are made to escalate privileges by users or applications.
- User session tracking – cloud platforms enable the monitoring of active user sessions and operations performed in real time.

Conclusion

Enterprises constantly use many identities assigned to users and specific services to perform daily business tasks, often involving the processing of critical data. Although identities are the primary access point to data and resources in the cloud, identity management has received very little attention. Identities are often configured with default security settings, and permissions are assigned without proper control.

Phishing tests conducted as part of the study showed that a significant number of user identities within organizations can be stolen and used to gain unauthorized access to data. This demonstrates the importance of implementing a security model based on multiple principles illustrated in this paper, where each security layer helps detect and block a cyberattack at a different stage of its execution. It is also important to highlight the role of monitoring, as few enterprises pay sufficient attention to it, even though it is an effective tool for detecting suspicious activities in cloud environments and identifying unauthorized use of identities and data access.

In addition to applying technical measures and security principles, it is essential to educate users and administrators by raising their awareness of potential attack methods, associated risks, and effective protection techniques. Together, these actions form the foundation of secure identity and access management in public cloud environments.

References

- Al-Qtiemat, E. and Al-Odat, Z. (2024) 'Examining Cloud Security: Identifying Risks and the Implemented Mitigation Strategies', *Journal of Theoretical and Applied Information Technology*, 102.
- Eurostat (2023), Cloud computing – statistics on the use by enterprises. [Online], [Retrieved 20 October 2025], https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises
- Eurostat (2025), Employed persons working from home by professional status – % of total employment. [Online], [Retrieved 20 October 2025], https://ec.europa.eu/eurostat/databrowser/view/lfsa_ehomp__custom_12158505/default/table
- Google Cloud (2023), Shared responsibilities and shared fate on Google Cloud. [Online], [Retrieved 20 October 2025], https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate
- Google Cloud (2024), Threat Horizons: H1 2024 Threat Horizons Report. [Online], [Retrieved 20 October 2025], https://services.google.com/fh/files/misc/threat_horizons_report_h12024.pdf
- Grassi, P.A., Fenton, J.L., Choong, Y-Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R. and Richer, J.P. (2025), Digital Identity Guidelines: Authentication and Authenticator Management, NIST Special Publication 800-63B-4. [Online], [Retrieved 20 October 2025], https://doi.org/10.6028/NIST.SP.800-63B-4
- Gumiński, M. et al. (2023) Information Society in Poland in 2023. Warsaw: Statistics Poland (GUS).
- Liang, X. and Xu, Y. (2025) 'A novel framework to identify cybersecurity challenges and opportunities for organizational digital transformation in the cloud', *Computers & Security*, 151.
- Łąka, P. (2024) 'Authentication and IAM (Identity and Access Management) Systems', in: Sajdak, M. (ed.) Introduction to IT Security. Vol. 2. Kraków: Securitum, 613–645.
- Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, NIST Special Publication 800-207. [Online], [Retrieved 20 October 2025], https://doi.org/10.6028/NIST.SP.800-207
- Suleski, T. et al. (2023) 'A review of multi-factor authentication in the Internet of Healthcare Things', *Digital Health*.