CyberBulwork

HUMAN FACTORS REPORT

February, 2025

Table of Contents

List of Figures

List of Tables

Executive Summary

Cybersecurity remains a critical concern in today's digital landscape, with human factors playing a pivotal role in both mitigating and exacerbating security risks. This report examines the human factor threat profile, emphasizing how human behavior, insider threats, poor security awareness, and access management challenges contribute to cybersecurity vulnerabilities. It also provides case studies, security awareness initiatives, and strategic recommendations to enhance Cyberbulwork's overall security posture.

One of the primary findings is the prevalence of phishing and social engineering attacks. Cybercriminals exploit human psychology to deceive employees into revealing sensitive information, making phishing one of the most common and effective cyber threats. Insider threats also pose a significant risk, whether through negligence, malicious intent, or credential compromise. Weak access controls and privilege misuse further increase vulnerability, as poorly managed permissions, failure to revoke access, and excessive privileges create opportunities for unauthorized entry. Additionally, a lack of cybersecurity awareness among employees contributes to inadvertent breaches and security lapses, highlighting the need for continuous training.

The rise of remote work and hybrid workforce models introduces new security challenges, including insecure connections, personal device usage, and greater exposure to cyber threats. Third-party and supply chain vulnerabilities also present risks, as partner organizations and vendors with weak security measures can serve as entry points for attackers. Human error and employee burnout exacerbate security risks, as overworked employees are more prone to mistakes such as mishandling sensitive data or falling for phishing scams. The use of unauthorized IT solutions, commonly referred to as shadow IT, further increases exposure to cyber threats by circumventing established security protocols.

A key case study examined in this report is Cyberbulwork's experience with the LockBit 2.0 ransomware group, which demonstrated how human factor vulnerabilities can contribute to major security breaches. The attack was facilitated by insider threats, weak access controls, and social engineering tactics. While Cyberbulwork managed to mitigate financial losses through proactive security measures and data backups, the incident underscored the importance of continuous security training, strong access control policies, and improved incident response capabilities.

To address these issues, Cyberbulwork implemented a security awareness program through the Wizer platform, incorporating role-based training, phishing simulations, and interactive learning modules. An accessibility audit was also conducted to ensure that training materials were inclusive and compliant with best practices. The findings from this audit revealed issues such as missing video captions, low contrast ratios, and poor keyboard navigation, which were subsequently addressed to enhance usability.

In addition to security awareness training, Cyberbulwork took a major step in improving authentication security by integrating **Single Sign-On (SSO) with Azure Active Directory (Azure AD)**. This measure significantly enhanced security by eliminating password fatigue, enforcing multi-factor authentication (MFA), and streamlining access management, ultimately reducing the risk of unauthorized access.

To further strengthen cybersecurity resilience, Cyberbulwork must implement several key strategies. Ongoing cybersecurity training and phishing simulations should be conducted to improve awareness and reinforce secure behaviors. Engaging employees through gamification and recognition programs will foster a proactive security culture. Strengthening communication strategies, including multi-channel security bulletins, phishing alerts, and executive messaging, will keep employees informed and vigilant. Enhancing access control measures through **Zero Trust security models, least-privilege access policies, and AI-powered threat detection** will further secure sensitive systems and data. Continuous security audits and red team exercises should be conducted to proactively identify and mitigate vulnerabilities before they are exploited by attackers.

Cybersecurity is not a one-time effort but a continuous, organization-wide initiative that requires awareness, leadership commitment, and adaptive defense mechanisms. By embedding security into daily operations, fostering a culture of shared responsibility, and leveraging advanced security technologies, Cyberbulwork can stay ahead of emerging cyber threats. Strengthening training programs, refining access controls, and enforcing robust security policies will ensure long-term resilience, enabling Cyberbulwork to safeguard its assets, reputation, and workforce in an ever-evolving threat landscape.

1.0 The Human Factor Threat Profile: Understanding the Weakest Link in Cybersecurity

In today's digital landscape, technology alone is not eno.0ugh to safeguard organizations from cyber threats. While firewalls, encryption, and intrusion detection systems play a vital role in security, human behavior remains the most unpredictable and vulnerable element. Cybercriminals recognize this and exploit human weaknesses to bypass even the most advanced security measures. Understanding the human factor threat profile is crucial for developing effective cybersecurity strategies.

1.1 Phishing and Social Engineering: Exploiting Human Trust

One of the most prevalent human-related threats is **phishing**, where attackers use deceptive emails, messages, or phone calls to manipulate individuals into revealing sensitive information, such as passwords or financial data. Unlike technical vulnerabilities, phishing attacks rely on human error, making them highly effective especially against organizations with low security awareness.

Similarly, **social engineering** tactics manipulate human psychology to gain unauthorized access. Attackers often impersonate trusted individuals, such as IT staff or executives, to trick employees into divulging confidential data or granting system access. These attacks are particularly dangerous because they bypass traditional security defenses and exploit an organization's greatest asset its people.

1.2 Insider Threats: The Risk from Within

While external attacks dominate cybersecurity discussions, **insider threats** can be even more damaging. Insiders whether malicious, negligent, or compromised already have legitimate access to sensitive systems and data, making it harder to detect their actions.

- **Malicious insiders** intentionally steal data, sabotage systems, or leak confidential information for financial gain, personal revenge, or corporate espionage.
- **Negligent insiders** inadvertently expose data or systems due to poor cybersecurity awareness, such as clicking on phishing links, using weak passwords, or mishandling sensitive documents.
- **Compromised insiders** are employees whose credentials have been stolen or who have been manipulated by cybercriminals, allowing attackers to infiltrate the organization undetected.

These threats highlight the need for strong **access controls, continuous monitoring, and employee education** to minimize risks.

1.3 Poor Password Management: A Gateway for Cybercriminals

Despite advancements in authentication technologies, weak password practices remain a major security concern. Many employees reuse passwords across multiple accounts, store them insecurely, or use easily guessable combinations. Attackers exploit this through **credential stuffing**, where stolen login details from one breach are used to access other accounts.

To combat this, organizations should enforce **multi-factor authentication (MFA)**, implement **password managers**, and regularly educate employees on secure password practices. Strengthening authentication methods can significantly reduce the risk of unauthorized access.

1.4 Lack of Cybersecurity Awareness: The Silent Threat

A workforce with inadequate cybersecurity awareness is a prime target for cybercriminals. Employees who are not trained to recognize threats may fall victim to scams, click on malicious links, or fail to report suspicious activity. This is particularly concerning as **attackers continuously evolve their tactics**, making traditional security training insufficient if not regularly updated.

Organizations must implement **continuous cybersecurity education**, using real-world simulations, phishing tests, and engaging training programs to reinforce security-conscious behavior. Building a **culture of security** ensures that employees act as the first line of defense rather than the weakest link.

1.5 Third-Party Risks: Security Beyond the Organization

Even with strong internal cybersecurity measures, organizations remain vulnerable to **third-party risks** security weaknesses introduced by vendors, contractors, or external partners. Many businesses rely on cloud services, software providers, and supply chains, all of which can be entry points for attackers.

A single breach in a third-party system can expose sensitive data or compromise an organization’s infrastructure. To mitigate this, companies should **conduct regular security audits, enforce strict access controls, and require vendors to comply with cybersecurity standards** before granting access to critical systems.

1.6 Human Error: The Root Cause of Most Cybersecurity Incidents

Human error, often influenced by workplace stress, distractions, or lack of proper training, remains a leading cause of security incidents. Employees under pressure may accidentally click on malicious links, misconfigure systems, or forget to follow security protocols. These seemingly minor mistakes can have devastating consequences, leading to data breaches, financial losses, and reputational damage.

To reduce human error, organizations must balance **security measures with usability**, ensuring that employees can perform their tasks efficiently without bypassing security protocols. Simplified security processes, automated safeguards, and intuitive security tools can help minimize risks while maintaining productivity.

1.7 Building a Human-Centric Cybersecurity Strategy

Addressing human factor threats requires more than just technology it demands a **holistic approach** that prioritizes **security awareness, strong policies, and proactive monitoring**. Key strategies include:

- **Security Awareness Training** – Regular and engaging training to educate employees about evolving cyber threats.
- **Zero Trust Security Model** – A security framework where no user or device is trusted by default.
- **Least Privilege Access** – Restricting access rights based on job roles to minimize risk.
- **Behavioral Monitoring** – Using AI-driven tools to detect unusual or suspicious activity.
- **Incident Response Plans** – Having a clear protocol for identifying, reporting, and mitigating security breaches.

By fostering a **cybersecurity-conscious culture**, organizations can transform their workforce from a security liability into a powerful defense mechanism. Recognizing the human factor in cybersecurity is not just about identifying risks it's about empowering individuals to be vigilant, responsible, and proactive in protecting their organization from cyber threats.

2.0 Top Human Factor Threats in the Consulting and IT Industry

Consulting and technology firms, such as Accenture, manage vast amounts of sensitive client data, intellectual property, and critical systems daily. While advanced security measures are in place, human error remains a significant cybersecurity vulnerability. Regardless of technological advancements, human factors continue to be a leading cause of security incidents—whether through accidental mistakes or intentional misconduct.

2.1 Key Human-Related Cybersecurity Threats in the Consulting and IT Industry

1. Insider Threats: Accidental & Malicious

Not all cyber threats come from external sources; some of the most significant risks originate within the organization.

- **Accidental Insiders**: Employees or contractors who unintentionally compromise security by mishandling sensitive data, misconfiguring systems, or falling victim to phishing attacks.
- **Malicious Insiders**: Individuals who exploit their access to steal data, sabotage systems, or leak confidential client information.

Example: A consultant leaves their laptop on public transport, exposing unencrypted client data to unauthorized access.

2. Phishing & Social Engineering Attacks

Cybercriminals exploit human psychology rather than technical vulnerabilities to gain access to systems.

- **Spear Phishing**: Highly targeted phishing attacks aimed at executives or IT administrators.
- **Business Email Compromise (BEC)**: Fraudsters impersonate corporate leaders to trick employees into transferring money or disclosing sensitive information.

Example: A consultant receives an email appearing to be from a manager, requesting urgent review of an "important document," which turns out to be malware.

3. Weak Access Controls & Privilege Misuse

Granting excessive access rights can increase security risks.

- Overprivileged accounts make it easier for attackers to inflict damage if compromised.
- Poor offboarding practices can leave former employees with lingering access to critical systems.

Example: A former consultant's credentials remain active months after leaving the company, posing a security risk.

4. Lack of Cybersecurity Awareness & Training

Employees unaware of security best practices can unknowingly create vulnerabilities.

- Weak password practices and password reuse across multiple accounts.
- Ignoring security alerts or failing to recognize suspicious behavior.

Example: A consultant uses the same weak password for multiple business accounts, making them an easy target for attackers.

5. Remote Work & Hybrid Workforce Risks

The shift to remote work has introduced new security challenges.

- Misconfigured cloud storage solutions (e.g., Google Drive, SharePoint) leading to unintended data leaks.
- Employees bypassing security protocols for convenience.

Example: A remote consultant connects to a client system using public Wi-Fi, unknowingly exposing sensitive data.

6. Third-Party & Supply Chain Vulnerabilities

Consulting firms rely on vendors, partners, and subcontractors, many of whom may have weaker security measures.

Example: A smaller IT vendor working with Accenture is breached, and attackers use their access to infiltrate Accenture's internal systems.

7. Employee Burnout & Human Error

Overworked employees are more likely to make security mistakes.

- Ignoring security alerts or circumventing security controls due to fatigue.
- Sending sensitive data to the wrong recipient due to distraction.

Example: A fatigued consultant accidentally uploads confidential client data to a public file-sharing service instead of a secure platform.

8. Poor Incident Response Awareness

Employees who do not know how to report security incidents can allow threats to persist.

Example: A consultant notices unusual login attempts but ignores them, giving attackers prolonged access.

9. Shadow IT & Unauthorized Software Use

Employees using unauthorized applications or personal devices for work introduce security risks.

- Storing sensitive data on unapproved cloud services.
- Using unprotected personal devices for work tasks.

Example: A consultant uses an AI-powered writing tool that unknowingly stores confidential client data on external servers.

10. Ethical & Compliance Violations

Consulting firms must adhere to strict ethical and regulatory standards when handling client data.

Example: A consultant shares confidential client information with a third-party vendor without proper authorization, leading to a data breach.

Despite technological advancements, human factors remain one of the most significant cybersecurity challenges in the consulting and IT industry. Organizations must prioritize security awareness training, enforce strict access controls, and implement robust incident response plans to mitigate these risks.

3.0 Case Study: Cyberbulwork Under Hostage of LockBit 2.0 Group

3.1 Top Human Factor Threats in Cloud Infrastructure and IT Consulting Industries

Cybersecurity threats are not just technical but often stem from human-related vulnerabilities. Within cloud infrastructure and IT consulting, the following human factor threats pose significant risks:

- **Insider Threats** – Employees or contractors misusing access for malicious intent or negligence.
- **Phishing & Social Engineering Attacks** – Exploiting human trust to gain unauthorized access.
- **Weak Access Controls & Privilege Misuse** – Poorly managed permissions allowing unauthorized data access.
- **Lack of Cybersecurity Awareness & Training** – Employees unaware of best security practices.
- **Third-Party & Supply Chain Vulnerabilities** – Security gaps in vendors and partners impacting the organization.
- **Remote Work & Hybrid Workforce Risks** – Expanded attack surface due to remote connectivity.
- **Employee Burnout & Human Error** – Stress and fatigue leading to lapses in security.
- **Poor Incident Response Awareness** – Delays in recognizing and mitigating cyber threats.
- **Shadow IT & Unauthorized Software Use** – Unapproved applications increasing security risks.
- **Ethical & Compliance Violations** – Failure to adhere to security policies and regulations.

3.2 Cyberbulwork's AWS S3 Bucket Vulnerability (2017)

In 2017, Cyberbulwork suffered a significant data exposure when four AWS S3 storage buckets were left publicly accessible. These buckets contained sensitive credentials and client information. The root cause was inadequate access control reviews and misconfigurations, emphasizing the role of human error in cloud security lapses.

3.3 Human Factors Behind the 2021 Cyberbulwork Data Breach

In August 2021, Cyberbulwork was targeted by the LockBit 2.0 ransomware group. Although the company downplayed the impact, cybersecurity analysts pointed to human-related vulnerabilities as key contributors to the breach. The primary human factors included:

- **Insider Threats** – Potential internal actors aiding or neglecting security protocols.
- **Poor Access Controls & Privilege Management** – Excessive access rights increasing risk exposure.
- **Social Engineering** – Attackers manipulating employees to gain entry.

- **Failure in Employee Awareness & Reporting** – Lack of vigilance in recognizing suspicious activity.

3.4 Impact of the Ransomware Attack on Cyberbulwork and Stakeholders

Cyberbulwork's breach mirrored other high-profile attacks, such as Capgemini's REvil incident and IBM's indirect Clop Group exposure. The consequences were far-reaching:

A. Impact on Cyberbulwork

- **Reputation Damage** – As an IT and cybersecurity firm, higher security expectations led to credibility concerns.
- **Operational Disruptions** – Despite claims of minimal impact, internal operations faced disruptions.
- **Intellectual Property & Financial Losses** –
  - Costly forensic investigations and system restorations.
  - Legal expenses due to regulatory scrutiny.
  - LockBit 2.0 claimed theft of 6TB of data, demanding a $50 million ransom, though Cyberbulwork avoided payment due to reliable backups.

B. Impact on Stakeholders

- **Secondary Data Breach Risks** – Client and partner data potentially exposed.
- **Trust Issues** – Diminished confidence in Cyberbulwork's security capabilities.
- **Potential Supply Chain Attacks** – Increased vulnerabilities for clients and partners.
- **Personal Data Exposure** – Employees and customers at risk of identity theft.
- **Job Security Concerns** – Fear of layoffs due to financial strain.
- **Stock Stability** – Market trust remained intact despite the incident.
- **Regulatory & Legal Scrutiny** – Compliance violations led to investigations.
- **Demonstration of LockBit's Sophistication** – The attack underscored the evolving threat landscape.

5. Cyberbulwork's Response to the Incident

Cyberbulwork's crisis response was swift and strategic:

- **Isolation & Containment** – Affected systems were quickly quarantined.

- **Backup Recovery** – Restoration from backups minimized downtime.
- **Transparent Communication** – Stakeholders were reassured about the limited impact and non-payment of ransom.
- **Enhanced Security Measures** – Strengthened defenses post-attack to prevent recurrence.
- **Collaboration with Authorities** – Worked with cybersecurity agencies and regulators to investigate and track perpetrators.

6. Lessons Learned

The Cyberbulwork case highlights critical cybersecurity takeaways:

- **Human Factors Are a Major Risk** – Even cybersecurity experts are vulnerable to insider threats, social engineering, and access mismanagement.
- **Proactive Security Measures Matter** – Cyberbulwork's data backup strategy prevented more severe consequences.
- **Incident Response Plans Are Essential** – Rapid system restoration demonstrated the value of preparedness.
- **Continuous Security Training is Necessary** – Employees must be educated to recognize and respond to threats effectively.

4.0 Security Awareness Program Design

In today’s rapidly evolving digital landscape, human error remains one of the most significant vulnerabilities in cybersecurity. To address this challenge, Cyberbulwork launched a **Security Awareness Program** designed to educate and empower employees against cyber threats. This initiative, delivered through the **Wizer training platform**, provides structured, role-based learning to help staff recognize and mitigate potential risks.

The training modules were **strategically curated based on the human-factor threats identified during our cyber threat intelligence sprint**, ensuring a targeted approach to addressing real security gaps within the organization. These threats included insider risks, phishing and social engineering attacks, weak access controls, and security lapses due to remote work. By focusing on these high-risk areas, the program enhances overall security hygiene while reinforcing best practices.

Through interactive training modules, quizzes, and continuous monitoring, Cyberbulwork aims to build a security-conscious workforce that actively defends against cyber threats.

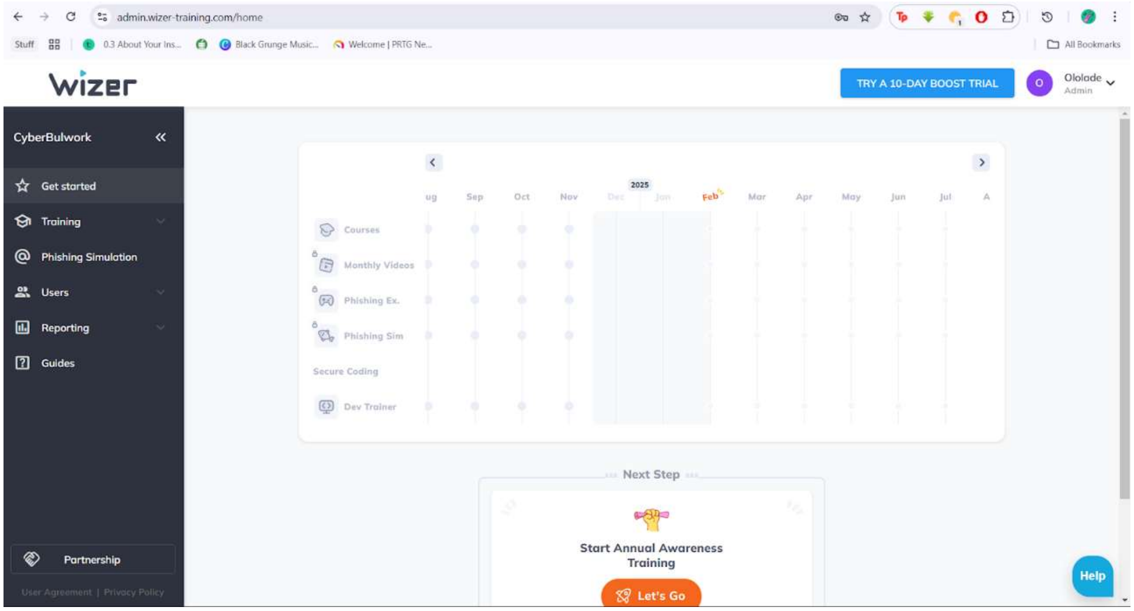
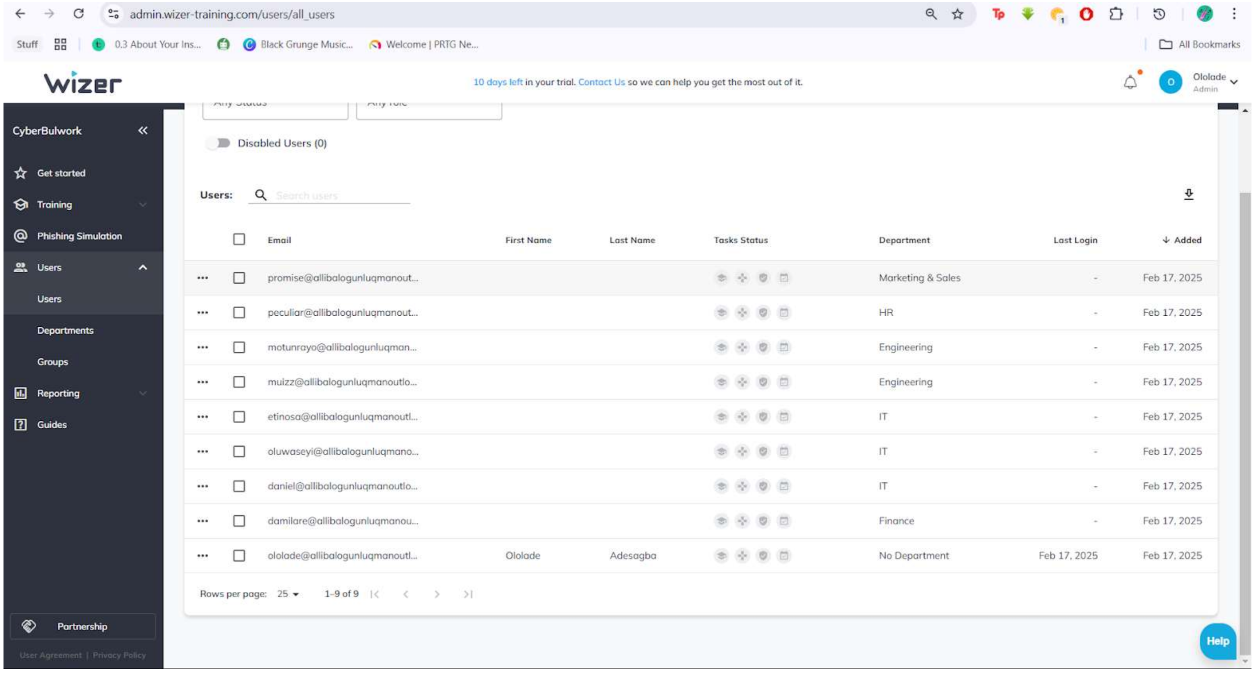


Figure 1: CyberBulwork Wizer platform



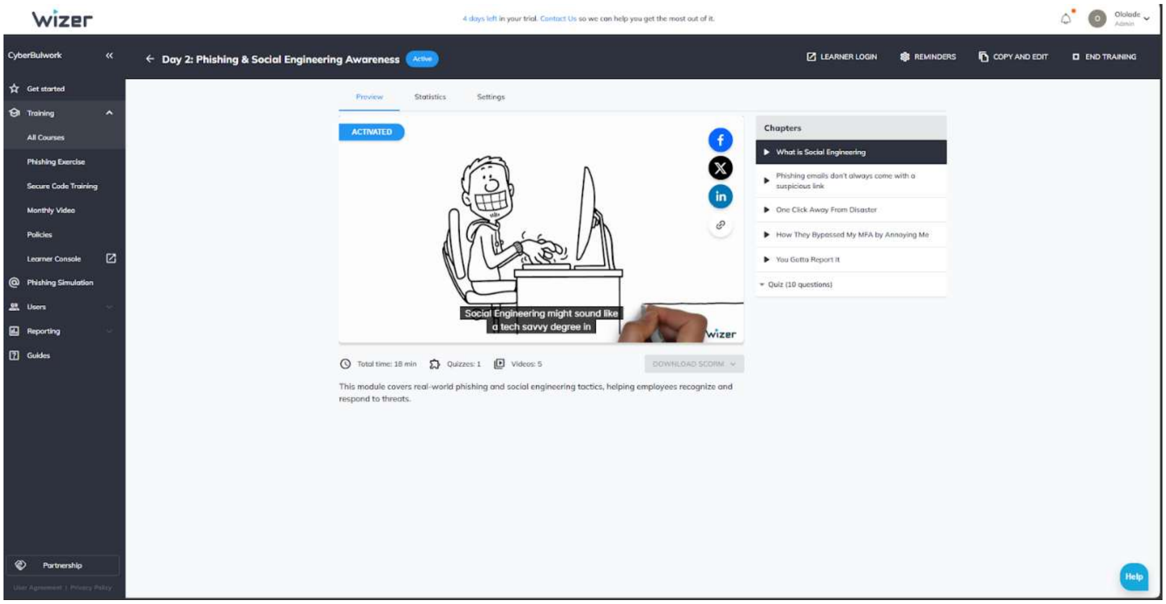
10 days left in your trial. Contact Us so we can help you get the most out of it.

	Email	First Name	Last Name	Tasks Status	Department	Last Login	↓ Added
☐	promise@allibalogunluqmanout...				Marketing & Sales	-	Feb 17, 2025
☐	peculiar@allibalogunluqmanout...				HR	-	Feb 17, 2025
☐	motunrayo@allibalogunluqman...				Engineering	-	Feb 17, 2025
☐	muizz@allibalogunluqmanoutlo...				Engineering	-	Feb 17, 2025
☐	etinosa@allibalogunluqmanoutl...				IT	-	Feb 17, 2025
☐	oluwaseyi@allibalogunluqmano...				IT	-	Feb 17, 2025
☐	daniel@allibalogunluqmanoutlo...				IT	-	Feb 17, 2025
☐	damilare@allibalogunluqmanou...				Finance	-	Feb 17, 2025
☐	ololade@allibalogunluqmanoutl...	Ololade	Adesagba		No Department	Feb 17, 2025	Feb 17, 2025

Rows per page: 25 1-9 of 9

Figure 2: Staff Onboarding on CyberBulwork

Figure 1 illustrates the creation of the Cyberbulwork account on the Wizer platform, marking the foundation of the security awareness program. **Figure 2** captures the staff onboarding process, ensuring employees are enrolled and ready to engage with the training. **Figure 3** showcases one of the curated courses designed to address human factor threats identified during our cyber threat intelligence sprint. **Figure 4** presents the response rates of these courses, reflecting staff engagement and participation levels in the program.



4 days left in your trial. Contact Us so we can help you get the most out of it.

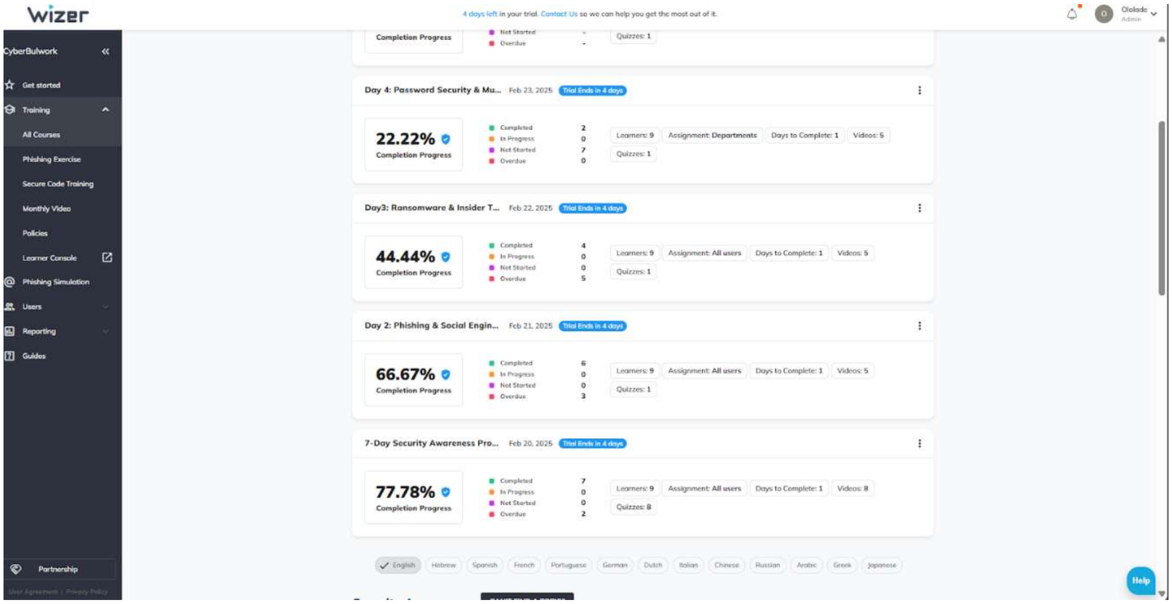
Day 2: Phishing & Social Engineering Awareness

Chapters
- What is Social Engineering
- Phishing emails don't always come with a suspicious link
- One Click Away From Disaster
- How They Bypassed My MFA by Annoying Me
- You Gotta Report It
- Quiz (10 questions)

Total time: 18 min Quizzes: 1 Videos: 5

This module covers real-world phishing and social engineering tactics, helping employees recognize and respond to threats.

Figure 3: One of the created courses



Completion Progress
Not Started -
Overdue -
Quizzes: 1

Day 4: Password Security & Mu... Feb 23, 2025 Trial Ends in 4 days

22.22% Completion Progress

Completed	2
In Progress	0
Not Started	7
Overdue	0

Learners: 9 | Assignment: Departments | Days to Complete: 1 | Videos: 5 | Quizzes: 1

Day3: Ransomware & Insider T... Feb 22, 2025 Trial Ends in 4 days

44.44% Completion Progress

Completed	4
In Progress	0
Not Started	0
Overdue	5

Learners: 9 | Assignment: All users | Days to Complete: 1 | Videos: 5 | Quizzes: 1

Day 2: Phishing & Social Engin... Feb 21, 2025 Trial Ends in 4 days

66.67% Completion Progress

Completed	6
In Progress	0
Not Started	0
Overdue	3

Learners: 9 | Assignment: All users | Days to Complete: 1 | Videos: 5 | Quizzes: 1

7-Day Security Awareness Pro... Feb 20, 2025 Trial Ends in 4 days

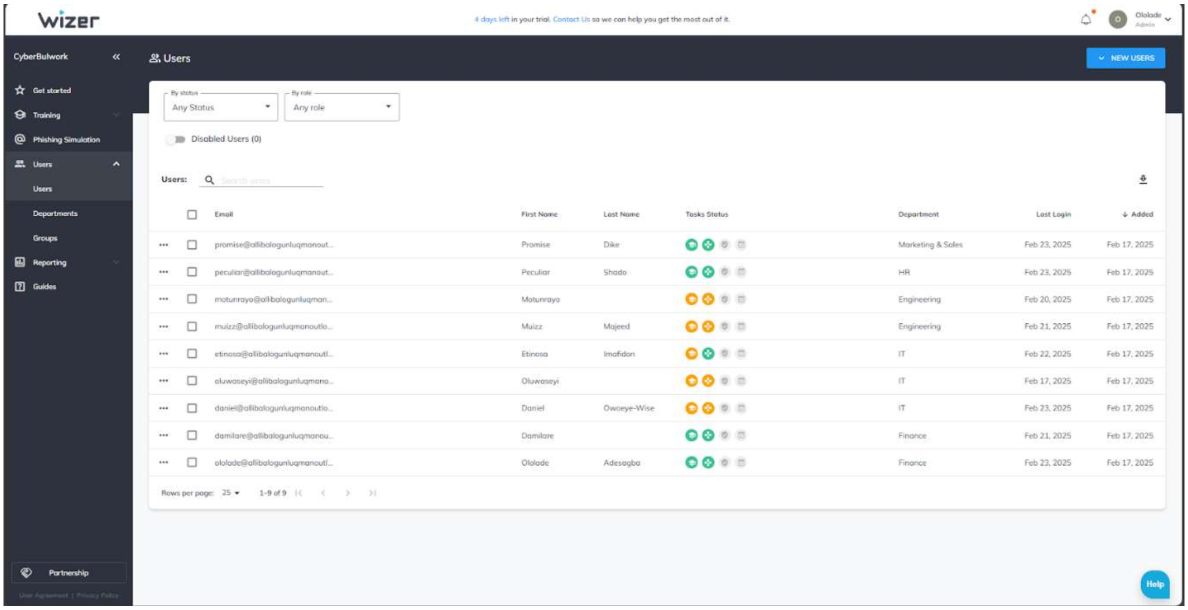
77.78% Completion Progress

Completed	7
In Progress	0
Not Started	0
Overdue	2

Learners: 9 | Assignment: All users | Days to Complete: 1 | Videos: 8 | Quizzes: 8

✓ English | Hebrew | Spanish | French | Portuguese | German | Dutch | Italian | Chinese | Russian | Arabic | Greek | Japanese

Figure 4: Response rates of the created courses for the cybersecurity program



By status: Any Status
By role: Any role
Disabled Users (0)

Users:

☐	Email	First Name	Last Name	Tasks Status	Department	Last Login	↓ Added
☐	promise@allibalogunluqmanout...	Promise	Dike	🟢 🟢	Marketing & Sales	Feb 23, 2025	Feb 17, 2025
☐	peculiar@allibalogunluqmanout...	Peculiar	Shado	🟢 🟢	HR	Feb 23, 2025	Feb 17, 2025
☐	motunrayo@allibalogunluqman...	Motunrayo		🟠 🟠	Engineering	Feb 20, 2025	Feb 17, 2025
☐	muizz@allibalogunluqmanoutlo...	Muizz	Majeed	🟠 🟠	Engineering	Feb 21, 2025	Feb 17, 2025
☐	etinosa@allibalogunluqmanoutl...	Etinosa	Imafidon	🟠 🟢	IT	Feb 22, 2025	Feb 17, 2025
☐	oluwaseyi@allibalogunluqmano...	Oluwaseyi		🟠 🟠	IT	Feb 17, 2025	Feb 17, 2025
☐	daniel@allibalogunluqmanoutlo...	Daniel	Owoeye-Wise	🟠 🟠	IT	Feb 23, 2025	Feb 17, 2025
☐	damilare@allibalogunluqmanou...	Damilare		🟢 🟢	Finance	Feb 21, 2025	Feb 17, 2025
☐	ololade@allibalogunluqmanoutl...	Ololade	Adesogba	🟢 🟢	Finance	Feb 23, 2025	Feb 17, 2025

Rows per page: 25 1-9 of 9

Figure 5: Wizer training completion dashboard

To maintain high engagement and reinforce cybersecurity best practices, each training module incorporated interactive elements, such as real-world attack scenarios and knowledge assessments. These assessments not only measure employees' understanding but also help identify areas where additional focus is needed.

Regular progress evaluations ensure that cybersecurity awareness remains a continuous effort at Cyberbulwork.

Understanding that cyber threats are constantly evolving, Cyberbulwork remains committed to updating its training materials to address emerging risks and industry best practices. This structured approach ensures that employees receive timely, relevant, and practical guidance, empowering them to recognize threats and take proactive security measures. By embedding cybersecurity awareness into its culture, Cyberbulwork strengthens its overall security posture and resilience against ever-changing cyber threats. The impact of this initiative is reflected in **Table 1** below:

Table 1: Cyberbulwork Security Awareness Content Release Schedule (6 Weeks)

Week	Training Module	Learning Objectives	Delivery Method	Assessment Type
Week 1	**Introduction to Cybersecurity Awareness**	Understand cybersecurity risks and their impact on daily operations.	Video + Quiz	Multiple-choice quiz
Week 2	**Phishing & Social Engineering Attacks**	Recognize phishing emails and manipulation tactics used by attackers.	Interactive Simulation	Scenario-based assessment
Week 3	**Ransomware & Malware Protection**	Identify malware threats and implement preventive measures.	Video + Case Studies	Knowledge check quiz
Week 4	**Multi-Factor Authentication & Access Control**	Apply MFA and proper access control to secure accounts.	Infographic + Video	Practical exercise
Week 5	**Insider Threats & Human Error Prevention**	Recognize accidental and malicious insider threats.	Video + Case Study	Scenario-based assessment
Week 6	**Remote Work & BYOD Security Best Practices**	Implement secure remote work policies and protect personal devices used for work.	Video + Policy Guidelines	Compliance checklist

Effective communication is critical to the success of Cyberbulwork's security awareness program. Without consistent engagement and reinforcement, employees may overlook key cybersecurity principles, leaving the organization vulnerable to threats. This communication strategy is designed to ensure that security awareness remains a continuous and interactive process rather than a one-time training event.

By leveraging multiple communication channels, tailored messaging, and strategic engagement methods, Cyberbulwork aims to create a culture where security is a shared responsibility. This approach will not only improve training completion rates but also empower employees to recognize and respond to cyber threats effectively. The following strategy outlines how Cyberbulwork will deliver security awareness messages, engage staff, and monitor the effectiveness of the program.

Table 2: Cyberbulwork Security Awareness Communication Strategy

Communication Channel	Purpose	Frequency	Responsible Team
Email Campaigns	Announce training, send reminders, and share key tips.	Weekly	IT Security Team
Slack/Microsoft Teams	Provide quick security tips and discussion threads.	Twice a week	IT Security Team
Company Newsletter	Highlight security updates and success stories.	Monthly	Communications Team
Awareness Posters	Display cybersecurity tips in office spaces.	Quarterly	HR & IT Security
Webinars & Live Sessions	Deep dive into key security topics with Q&A.	Bi-Monthly	IT Security Team
Simulated Phishing Emails	Assess and improve phishing awareness.	Every 2 months	IT Security Team

Table 3: Key Messaging Themes & Timeline

Week	Focus Area	Messaging Approach
Week 1	Introduction to Security Awareness	"Cyber threats are real. Stay alert, stay safe."
Week 2	Phishing & Social Engineering	"Think before you click – don't fall for phishing scams!"
Week 3	Ransomware & Malware Protection	"Protect your data – avoid malware traps."
Week 4	MFA & Access Control	"Stronger passwords, safer accounts— enable MFA today!"
Week 5	Insider Threats & Human Error Prevention	"Security starts with you; recognize insider threats."
Week 6	Remote Work & BYOD Security	"Work securely anywhere—follow remote security best practices."

4.1 Security Risk Behaviors

As cybersecurity threats rise, human behavior is crucial in protecting cyberbulwork's sensitive information. Many security risks stem from unintentional employee actions, which can lead to data breaches, account compromises, or financial fraud. As part of our security awareness initiative, we added a section to help employees understand various security risk behaviors, their potential impact, and best prevention practices. This awareness will serve as an educational tool to promote safe security practices within the organization.

Table 4: Cyberbulwork Security Awareness on Security Risk Behaviors

Security Risk	Behaviors	Preventive Strategies
Data Leak	• Improperly configuring cloud storage	• Secure configuration • Encryption of sensitive data

	• Unauthorized sharing of confidential files	• Verify emails, links, and unexpected requests.
Data Theft	• Leaving devices unlocked or unattended • Falling for phishing attacks that steal credentials	• Implement the least privileged access • Enable data loss prevention
Personal Exposure	• Oversharing personal information on social media • Using the same email and password across multiple sites	• Check social media settings and limit who sees your post • Enable two-factor Authentication
Physical Damage	• Mishandling or losing devices containing sensitive data • Not using screen locks or biometric authentication	• Report hazards • Follow organization protocol • Lock all devices
Privacy Violation	• Installing apps without checking privacy policies • Granting unnecessary permissions to apps and websites	• Encrypt sensitive emails and files • Shred confidential documents
Fraud & Identity Theft	• Not monitoring bank statements and credit reports • Using weak passwords for financial accounts	• Monitor your social and bank accounts • Conduct personal awareness
Account Compromise	• Falling for social engineering attacks • Storing login credentials in unencrypted text files	• Use a strong and unique password. • Report suspicious activities.

4.2 Comprehensive Summary of Wizer Platform Design for Cyberbulwork

Training Implementation

Cyberbulwork's security awareness program was meticulously designed and implemented on the Wizer platform to provide a structured, engaging, and measurable learning experience. The training modules were developed based on insights from the cyber threat intelligence sprint, which identified key human factor threats. Using Wizer's custom training feature, each module was tailored to address specific risks while ensuring that employees remained engaged throughout the learning process. The training followed a structured content release schedule, introducing topics gradually to help employees build cybersecurity knowledge over time. Topics included phishing and social engineering, ransomware and malware protection, multi-factor authentication (MFA) and access control, insider threats and human error prevention, and remote work and BYOD security.

Notification and Certification

To ensure active participation, Cyberbulwork implemented an automated notification system that kept employees informed about upcoming training modules, deadlines, and security tips. Email campaigns, Slack/Microsoft Teams updates, and company newsletters played a key role in keeping staff engaged. Additionally, awareness posters and webinars further reinforced security best practices. Upon completing the training, employees received certificates, recognizing their commitment to cybersecurity awareness. This certification not only served as an incentive but also reinforced a culture of accountability and security consciousness within the organization.

Progress Monitoring

The Wizer platform's user dashboard provided real-time insights into staff engagement and progress. This feature allowed the IT Security team to track completion rates, monitor individual and team progress, and identify employees who had yet to complete their training. By leveraging these analytics, Cyberbulwork ensured that employees remained accountable, and targeted follow-ups could be conducted where necessary to improve participation and compliance.

Assessment and Learning Objectives

Each training module was designed with well-defined learning objectives to ensure employees understood the importance of cybersecurity and how to apply best practices in their daily tasks. At the end of each module, assessments were implemented to evaluate comprehension, measure retention, and identify areas requiring further reinforcement. The results from these assessments helped guide continuous improvements to the training curriculum, ensuring that future iterations of the program addressed knowledge gaps effectively.

Phishing Simulations and Practical Application

To reinforce theoretical learning, Cyberbulwork incorporated phishing simulations to assess employees' ability to recognize and respond to phishing attacks. These real-world exercises helped bridge the gap between knowledge and practical application, ensuring that employees could effectively apply their training in real-life scenarios. The insights gained from these simulations further informed training improvements and reinforced the organization's overall security posture.

Through a strategically structured security awareness program on Wizer, Cyberbulwork successfully fostered a culture of vigilance and responsibility among its employees. The combination of engaging training content, real-time progress tracking, proactive communication, and practical assessments ensured that security awareness became an ongoing learning journey rather than a one-time initiative. This comprehensive approach empowered employees to detect, prevent, and respond to cyber threats effectively, strengthening Cyberbulwork's overall defense against evolving security risks.

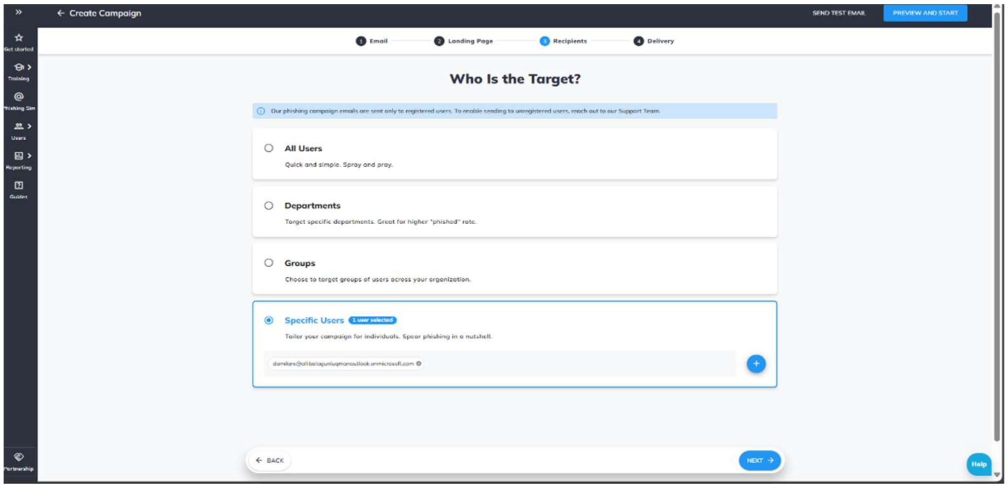
4.3 Developing a Phishing Simulation with Wizer

Phishing Simulation Campaign Exercise

Following the successful completion of our employee security awareness program, we conducted a phishing simulation campaign to assess whether participants had effectively retained the lessons from the training.

Results of the Phishing Simulation Campaign

The campaign data shows that all three recipients opened the phishing email, and only 2 of them clicked on the embedded link. Additionally, no reports of the phishing attempt were made. The simulation targeted two departments, Finance and Marketing, to evaluate employee awareness and test their ability to identify phishing threats.



Who Is the Target?

Our phishing campaign emails are sent only to registered users. To enable sending to unregistered users, reach out to our Support Team.

○ **All Users**
Quick and simple. Spray and pray.

○ **Departments**
Target specific departments. Great for higher "phished" rate.

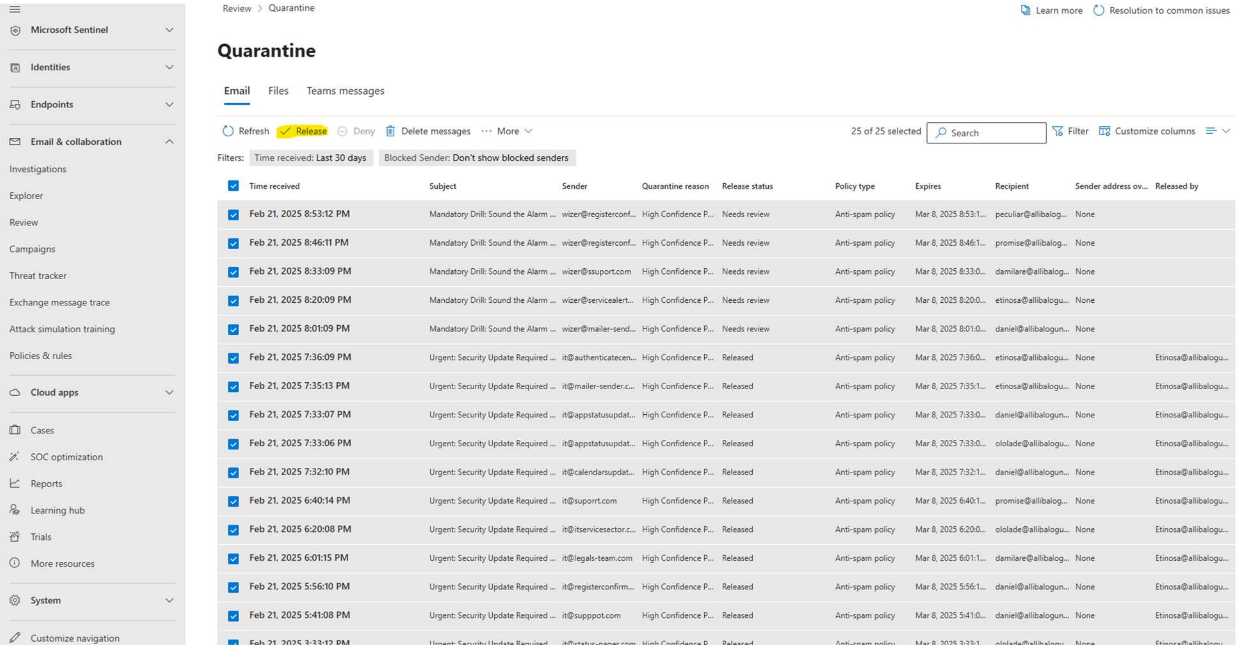
○ **Groups**
Choose to target groups of users across your organization.

● **Specific Users** 1 user selected
Tailor your campaign for individuals. Spear phishing in a nutshell.

damilare@allibalogunluqmanoutlook.onmicrosoft.com

Figure 6: Phishing simulation creation

The phishing simulation was designed to replicate real-world attack scenarios, ensuring that employees encountered emails resembling common phishing threats. The emails included suspicious links and urgent messaging tactics often used by cybercriminals.



Quarantine

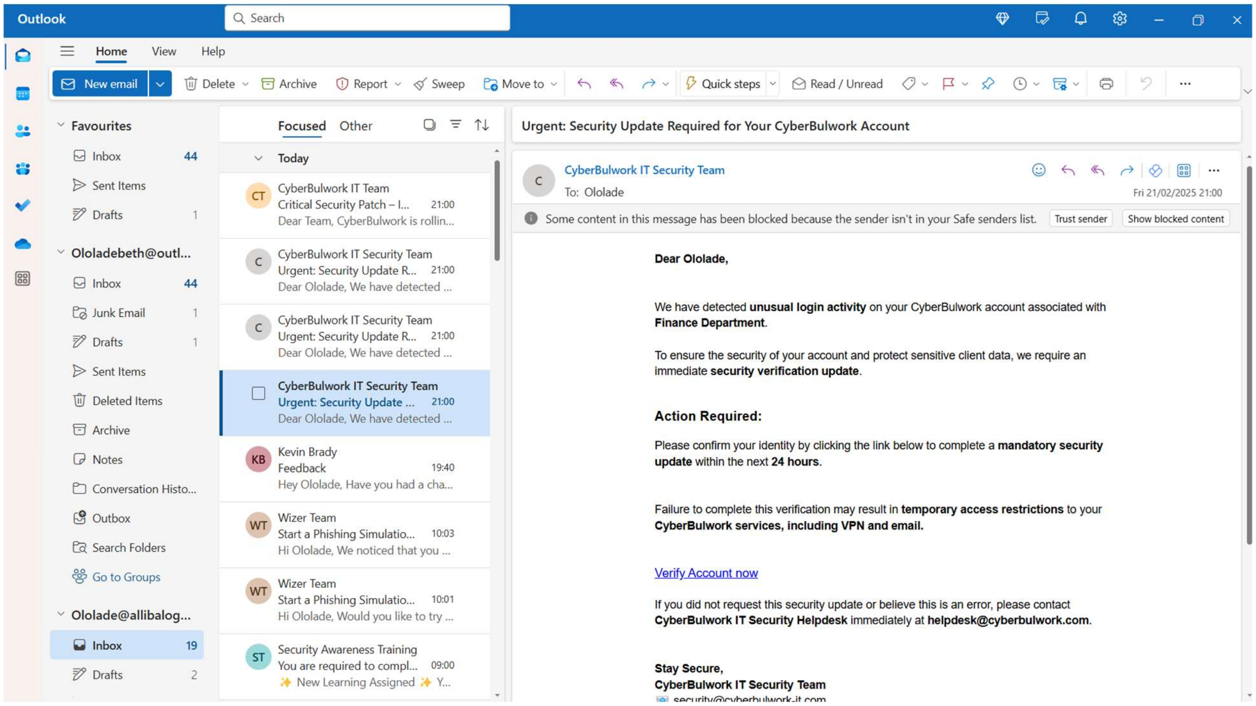
25 of 25 selected

Filters: Time received: Last 30 days | Blocked Sender: Don't show blocked senders

☑	Time received	Subject	Sender	Quarantine reason	Release status	Policy type	Expires	Recipient	Sender address ov...	Released by
☑	Feb 21, 2025 8:53:12 PM	Mandatory Drill: Sound the Alarm ...	wizer@registerconf...	High Confidence P...	Needs review	Anti-spam policy	Mar 8, 2025 8:53:1...	peculiar@allibalog...	None	
☑	Feb 21, 2025 8:46:11 PM	Mandatory Drill: Sound the Alarm ...	wizer@registerconf...	High Confidence P...	Needs review	Anti-spam policy	Mar 8, 2025 8:46:1...	promise@allibalog...	None	
☑	Feb 21, 2025 8:33:09 PM	Mandatory Drill: Sound the Alarm ...	wizer@ssuport.com	High Confidence P...	Needs review	Anti-spam policy	Mar 8, 2025 8:33:0...	damilare@allibalog...	None	
☑	Feb 21, 2025 8:20:09 PM	Mandatory Drill: Sound the Alarm ...	wizer@servicealert...	High Confidence P...	Needs review	Anti-spam policy	Mar 8, 2025 8:20:0...	etinosa@allibalogu...	None	
☑	Feb 21, 2025 8:01:09 PM	Mandatory Drill: Sound the Alarm ...	wizer@mailer-send...	High Confidence P...	Needs review	Anti-spam policy	Mar 8, 2025 8:01:0...	daniel@allibalogun...	None	
☑	Feb 21, 2025 7:36:09 PM	Urgent: Security Update Required ...	it@authenticatecen...	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 7:36:0...	etinosa@allibalogu...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 7:35:13 PM	Urgent: Security Update Required ...	it@mailer-sender.c...	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 7:35:1...	etinosa@allibalogu...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 7:33:07 PM	Urgent: Security Update Required ...	it@appstatusupdat...	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 7:33:0...	daniel@allibalogun...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 7:33:06 PM	Urgent: Security Update Required ...	it@appstatusupdat...	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 7:33:0...	ololade@allibalogu...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 7:32:10 PM	Urgent: Security Update Required ...	it@calendarsupdat...	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 7:32:1...	daniel@allibalogun...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 6:40:14 PM	Urgent: Security Update Required ...	it@suporrt.com	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 6:40:1...	promise@allibalog...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 6:20:08 PM	Urgent: Security Update Required ...	it@itservicesector.c...	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 6:20:0...	ololade@allibalogu...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 6:01:15 PM	Urgent: Security Update Required ...	it@legals-team.com	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 6:01:1...	damilare@allibalog...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 5:56:10 PM	Urgent: Security Update Required ...	it@registerconfirm...	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 5:56:1...	daniel@allibalogun...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 5:41:08 PM	Urgent: Security Update Required ...	it@supppot.com	High Confidence P...	Released	Anti-spam policy	Mar 8, 2025 5:41:0...	daniel@allibalogun...	None	Etinosa@allibalogu...
☑	Feb 21, 2025 3:33:12 PM	Urgent: Security Update Required	it@status-pager.com	High Confidence P	Released	Anti-spam policy	Mar 8, 2025 3:33:1	ololade@allibalogu	None	Etinosa@allibalogu

Figure 7: Quarantined mails

Despite the simulation, certain security measures were in place to detect and quarantine potential threats. However, some emails bypassed filters and reached recipients, demonstrating areas where security configurations could be further optimized



CT CyberBulwork IT Team
Critical Security Patch – I... 21:00
Dear Team, CyberBulwork is rollin...

C CyberBulwork IT Security Team
Urgent: Security Update R... 21:00
Dear Ololade, We have detected ...

C CyberBulwork IT Security Team
Urgent: Security Update R... 21:00
Dear Ololade, We have detected ...

CyberBulwork IT Security Team
Urgent: Security Update ... 21:00
Dear Ololade, We have detected ...

KB Kevin Brady
Feedback 19:40
Hey Ololade, Have you had a cha...

WT Wizer Team
Start a Phishing Simulatio... 10:03
Hi Ololade, We noticed that you ...

WT Wizer Team
Start a Phishing Simulatio... 10:01
Hi Ololade, Would you like to try ...

ST Security Awareness Training
You are required to compl... 09:00
✨ New Learning Assigned ✨ Y...

Urgent: Security Update Required for Your CyberBulwork Account

C CyberBulwork IT Security Team
To: Ololade
Fri 21/02/2025 21:00

Some content in this message has been blocked because the sender isn't in your Safe senders list. Trust sender Show blocked content

Dear Ololade,

We have detected **unusual login activity** on your CyberBulwork account associated with **Finance Department**.

To ensure the security of your account and protect sensitive client data, we require an immediate **security verification update**.

Action Required:

Please confirm your identity by clicking the link below to complete a **mandatory security update** within the next **24 hours**.

Failure to complete this verification may result in **temporary access restrictions** to your **CyberBulwork services, including VPN and email.**

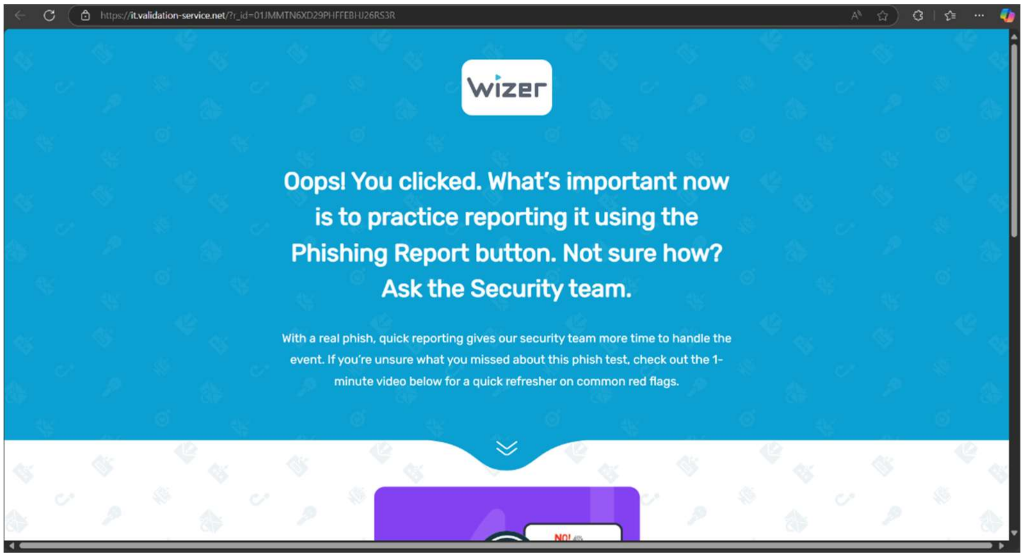
Verify Account now

If you did not request this security update or believe this is an error, please contact **CyberBulwork IT Security Helpdesk** immediately at **helpdesk@cyberbulwork.com**.

Stay Secure,
CyberBulwork IT Security Team
security@cyberbulwork-it.com

Figure 8: Phishing mail Delivered

The phishing email was successfully delivered to employees in the targeted departments. The email structure was designed to test their ability to recognize and respond appropriately to suspicious content.

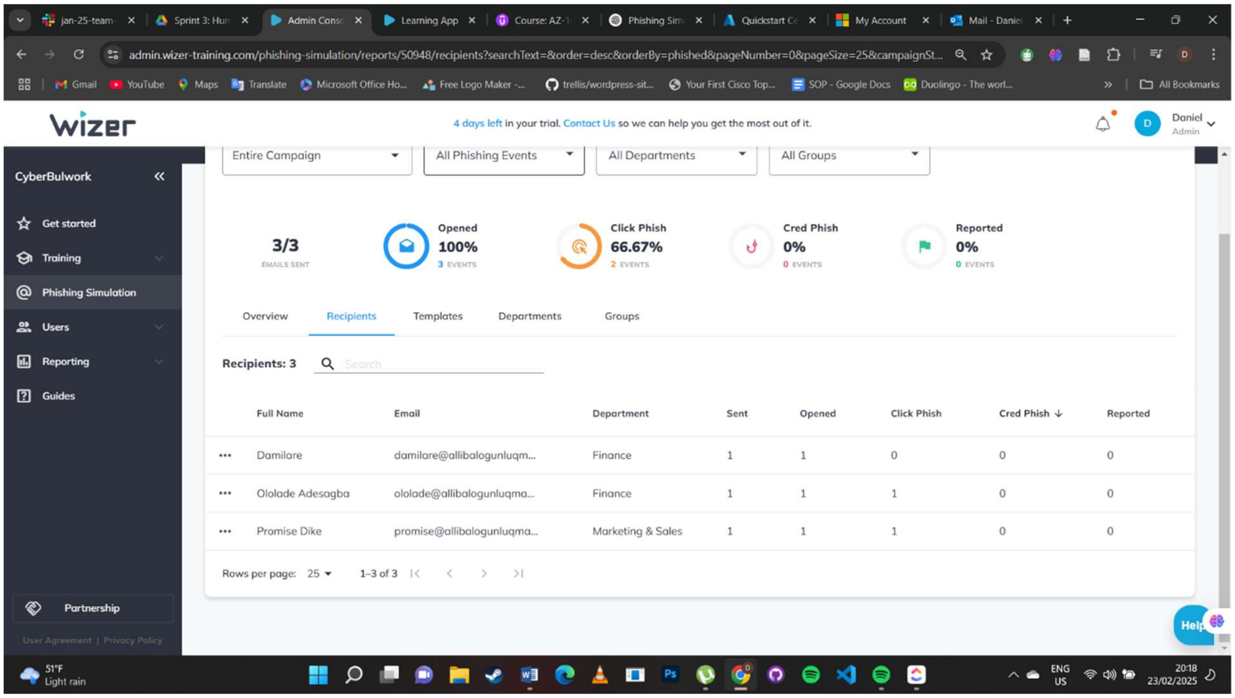

https://it.validation-service.net/?r_id=01JMMTN6XD29PHFFEBHJ26RS3R

Oops! You clicked. What's important now is to practice reporting it using the Phishing Report button. Not sure how? Ask the Security team.

With a real phish, quick reporting gives our security team more time to handle the event. If you're unsure what you missed about this phish test, check out the 1-minute video below for a quick refresher on common red flags.

Figure 9: Phishing link clicked

Two recipients engaged with the phishing attempt by clicking on the embedded link, highlighting the need for continuous awareness training and reinforcement of safe email practices.



3/3
EMAILS SENT

Opened 100% 3 EVENTS

Click Phish 66.67% 2 EVENTS

Cred Phish 0% 0 EVENTS

Reported 0% 0 EVENTS

Recipients: 3

Full Name	Email	Department	Sent	Opened	Click Phish	Cred Phish ↓	Reported
Damilare	damilare@allibalogunluqm...	Finance	1	1	0	0	0
Ololade Adesagba	ololade@allibalogunluqma...	Finance	1	1	1	0	0
Promise Dike	promise@allibalogunluqma...	Marketing & Sales	1	1	1	0	0

Rows per page: 25 1–3 of 3

Figure 10: Phishing simulation Completion

The simulation provided valuable insights into employee responses, allowing us to refine our security training programs and reinforce best practices for identifying phishing attempts.

Phishing simulation campaigns play a vital role in strengthening an organization’s cybersecurity posture by addressing the human factor, which is often the most vulnerable aspect of security defenses. These exercises offer several key benefits:

- **Enhancing Awareness and Education:** Employees gain firsthand experience in identifying phishing tactics used by cybercriminals. By interacting with simulated phishing scenarios, they become more adept at recognizing suspicious emails, links, and requests, reducing their risk of falling for actual scams.
- **Encouraging Behavioral Change:** Regular simulations reinforce good cybersecurity practices, helping employees develop a cautious approach when handling emails, attachments, and links, ultimately minimizing the chances of engaging with malicious content.

- **Assessing and Benchmarking Security Training:** These exercises provide a structured way to evaluate the effectiveness of security awareness training. Monitoring employee responses to simulated attacks helps identify vulnerabilities and track progress over time.
- **Reducing Security Risks:** By improving employees' ability to detect phishing attempts, organizations can significantly decrease the likelihood of data breaches, financial loss, and reputational harm associated with successful phishing attacks.
- **Meeting Compliance Requirements:** Many industries mandate cybersecurity awareness initiatives. Running phishing simulations helps organizations fulfill regulatory obligations and demonstrate their commitment to mitigating cyber threats.
- **Identifying At-Risk Employees:** Not all employees possess the same level of cybersecurity awareness. These simulations highlight individuals who may be more susceptible to phishing, enabling targeted training to enhance their security awareness.
- **Improving Incident Response Plans:** Observing employee reactions to phishing attempts allows organizations to refine their response strategies, ensuring a well-coordinated and effective approach to handling real cyber threats.

By regularly conducting phishing simulations, organizations can foster a security-conscious workforce, strengthen defenses against cyber threats, and enhance their overall cybersecurity resilience.

5.0 Accessibility Test

When we talk about cybersecurity, the conversation usually centers around protecting systems, networks, and data from malicious actors. But accessibility is an equally important piece that often goes unnoticed. Making cybersecurity accessible isn't just about compliance or ticking boxes; it's about ensuring that *everyone*, regardless of ability, has equal access to digital safety.

In a world where digital threats are constantly evolving, excluding people from essential security tools can put them, and even entire systems, at risk. So, what exactly does accessibility in cybersecurity mean, and why is it so important?

5.1 What is Accessibility in Cybersecurity?

At its core, **accessibility** in cybersecurity refers to designing and implementing security measures, tools, and practices that are usable by people of all abilities, including those with disabilities. This includes individuals with visual, auditory, cognitive, motor, or even temporary impairments. Think about it: if a two-factor authentication (2FA) app isn't compatible with a screen reader, how is a visually impaired user supposed to log in securely? Or if a critical security warning is delivered only as a flashing pop-up without any auditory cue, how will a user with visual impairments even notice it? Accessibility ensures that **no one** is left behind when it comes to securing their data and digital identities. It's about breaking down barriers and creating security solutions that *everyone* can use confidently.

To uphold our commitment to inclusivity and usability, the team conducted an accessibility assessment of key resources, including previously submitted PDF reports and security awareness training videos. The objective was to identify accessibility barriers and ensure these materials align with best practices. For the web accessibility evaluation, we utilized both the Axe DevTool and Lera, two highly regarded automated testing tools. As both tools generated identical results, we selected Lera for further analysis.

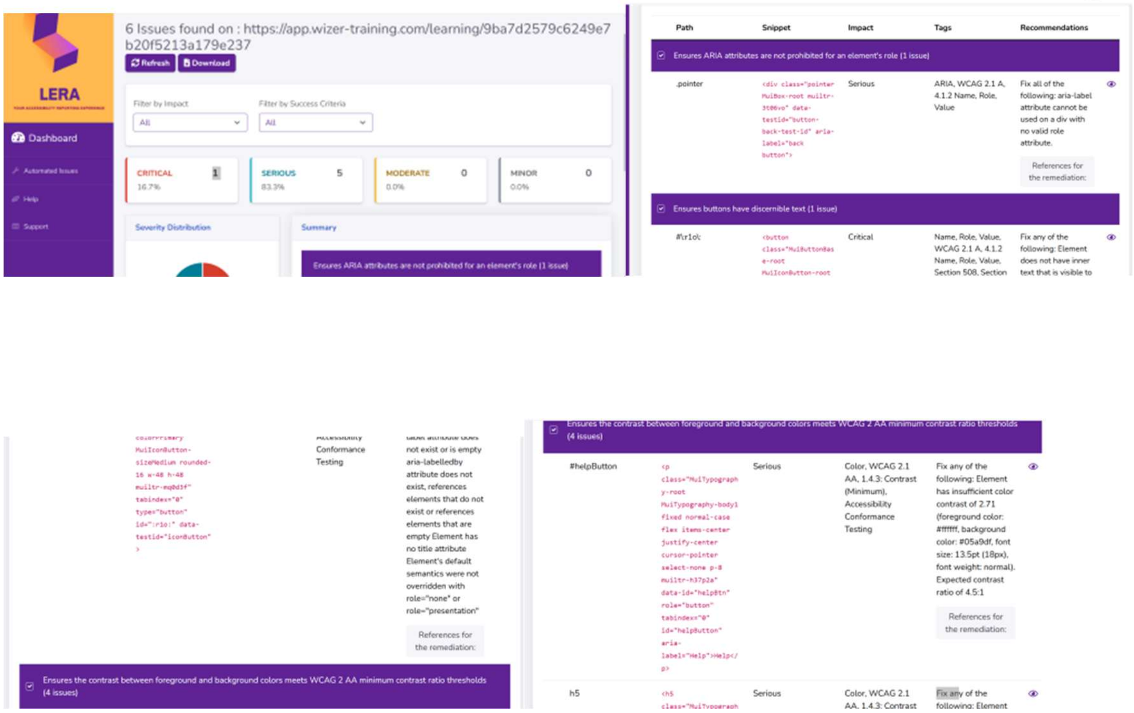
5.2 Web Accessibility Testing

For the web accessibility evaluation, we utilized both the Axe DevTool and Lera, two highly regarded automated testing tools. As both tools generated identical results, we selected Lera for further analysis.

5.3 Identified Accessibility Issues

The accessibility tests conducted on the **security awareness training videos** hosted on the **Wizer platform** revealed **three serious accessibility issues**:

1. **Lack of Proper Video Captions & Transcripts** – The videos did not include accurate closed captions or full transcripts, making them inaccessible to individuals with hearing impairments.
2. **Insufficient Color Contrast** – Certain UI elements within the video interface did not meet contrast ratio standards, making it difficult for users with visual impairments to distinguish text and background content.
3. **Keyboard Navigation Limitations** – Users relying on keyboard-only navigation faced difficulties accessing key controls, affecting individuals with motor impairments.



6 Issues found on : https://app.wizer-training.com/learning/9ba7d2579c6249e7b20f5213a179e237

Filter by Impact: All

Filter by Success Criteria: All

CRITICAL 1 16.7%

SERIOUS 5 83.3%

MODERATE 0 0.0%

MINOR 0 0.0%

Ensures ARIA attributes are not prohibited for an element's role (1 issue)

Path	Snippet	Impact	Tags	Recommendations
☑ Ensures ARIA attributes are not prohibited for an element's role (1 issue)				
.pointer	`<div class="pointer MuiBox-root muiltr-3t06vo" data-testid="button-back-test-id" aria-label="back button">`	Serious	ARIA, WCAG 2.1 A, 4.1.2 Name, Role, Value	Fix all of the following: aria-label attribute cannot be used on a div with no valid role attribute. References for the remediation:
☑ Ensures buttons have discernible text (1 issue)				
#\:r1o\:	`<button class="MuiButtonBase-root MuiIconButton-root`	Critical	Name, Role, Value, WCAG 2.1 A, 4.1.2 Name, Role, Value, Section 508, Section	Fix any of the following: Element does not have inner text that is visible to

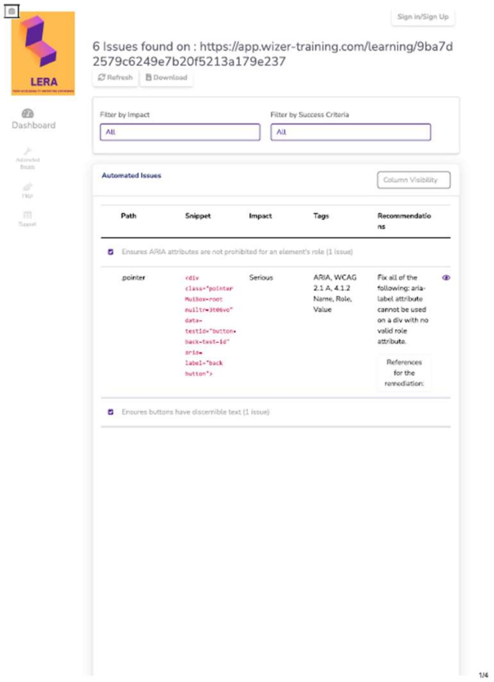
	`colorPrimary MuiIconButton-sizeMedium rounded-16 w-48 h-48 muiltr-mq0d3f" tabindex="0" type="button" id=":r1o:" data-testid="iconButton" >`		Accessibility Conformance Testing	label attribute does not exist or is empty aria-labelledby attribute does not exist, references elements that do not exist or references elements that are empty Element has no title attribute Element's default semantics were not overridden with role="none" or role="presentation" References for the remediation:
☑ Ensures the contrast between foreground and background colors meets WCAG 2 AA minimum contrast ratio thresholds (4 issues)				
#helpButton	`<p class="MuiTypography-root MuiTypography-body1 fixed normal-case flex items-center justify-center cursor-pointer select-none p-8 muiltr-h37p2a" data-id="helpBtn" role="button" tabindex="0" id="helpButton" aria-label="Help">Help</p>`	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast (Minimum), Accessibility Conformance Testing	Fix any of the following: Element has insufficient color contrast of 2.71 (foreground color: #ffffff, background color: #05a9df, font size: 13.5pt (18px), font weight: normal). Expected contrast ratio of 4.5:1 References for the remediation:
h5	`<h5 class="MuiTypograph`	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast	Fix any of the following: Element

Figure 11: Security Risk behavior analysis

Additionally, accessibility tests on **previously submitted PDF reports** identified formatting issues that could hinder readability for users relying on screen readers:

1. **Unreadable Text for Screen Readers** – Some PDF documents contained improperly tagged elements, preventing screen readers from interpreting content accurately.
2. **Missing Alternative Text for Images** – Essential diagrams and figures lacked alternative text descriptions, making the information inaccessible to visually impaired users.

3. **Navigation Challenges** – The structure of the PDFs did not follow logical reading order, causing difficulties for users with assistive technologies.



6 Issues found on : https://app.wizer-training.com/learning/9ba7d2579c6249e7b20f5213a179e237

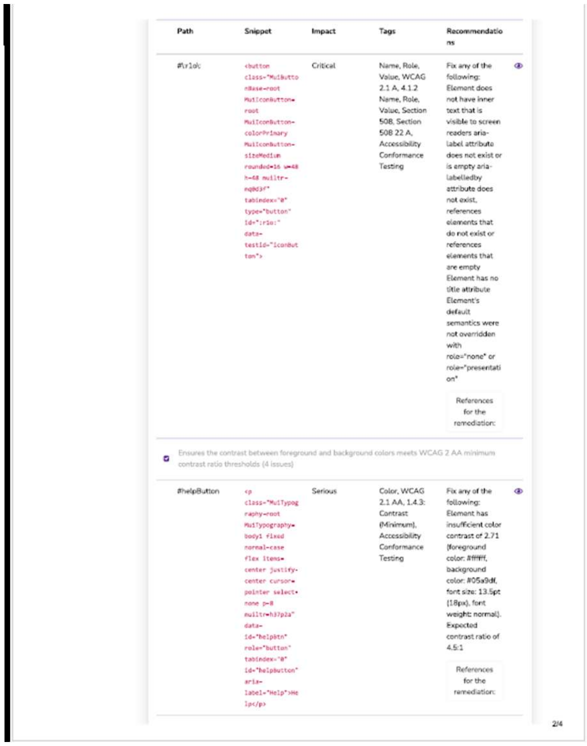
Filter by Impact: All

Filter by Success Criteria: All

Automated Issues

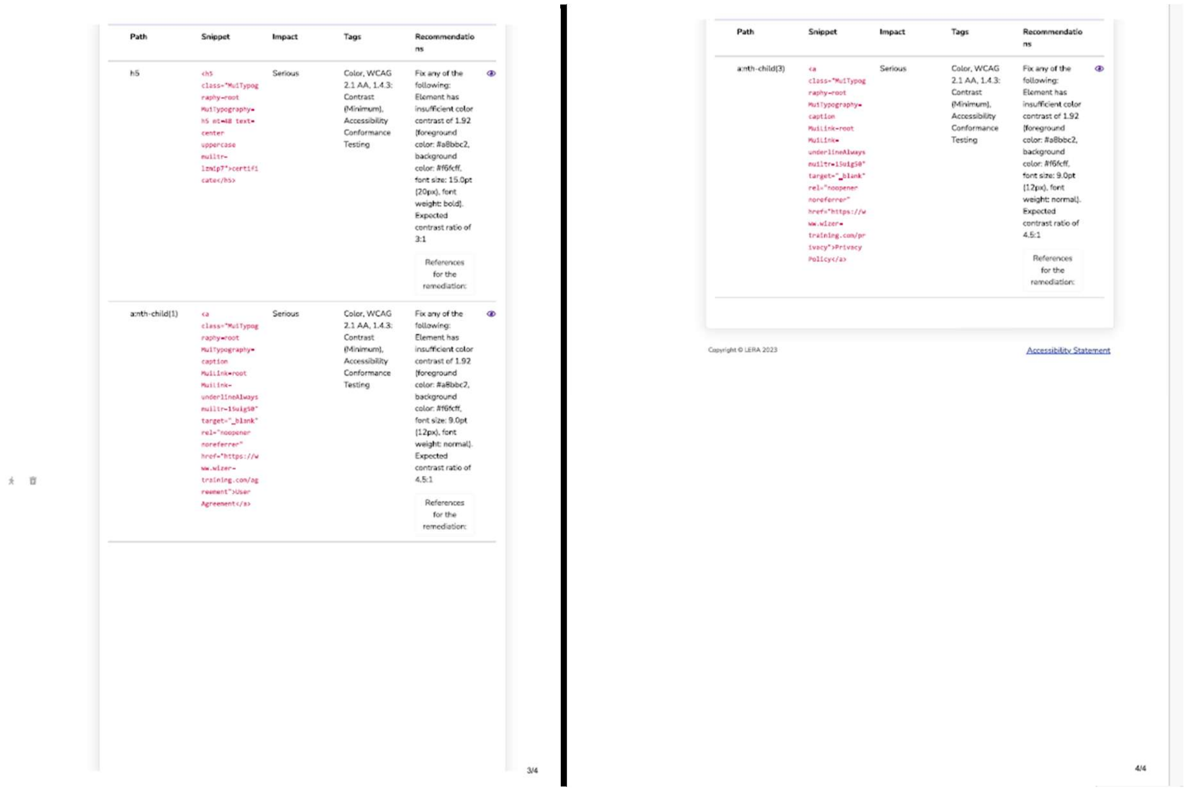
Path	Snippet	Impact	Tags	Recommendations
☑ Ensures ARIA attributes are not prohibited for an element's role (1 issue)				
.pointer	`<div class="pointer MuiBox-root muiltr-3t06vo" data-testid="button-back-test-id" aria-label="back button">`	Serious	ARIA, WCAG 2.1 A, 4.1.2 Name, Role, Value	Fix all of the following: aria-label attribute cannot be used on a div with no valid role attribute. References for the remediation:
☑ Ensures buttons have discernible text (1 issue)				

1/4



Path	Snippet	Impact	Tags	Recommendations
#\r1o\:	`<button class="MuiButtonBase-root MuiIconButton-root MuiIconButton-colorPrimary MuiIconButton-sizeMedium rounded-16 w-48 h-48 muiltr-mq0d3f" tabindex="0" type="button" id=":r1o:" data-testid="IconButton">`	Critical	Name, Role, Value, WCAG 2.1 A, 4.1.2 Name, Role, Value, Section 508, Section 508 22 A, Accessibility Conformance Testing	Fix any of the following: Element does not have inner text that is visible to screen readers aria-label attribute does not exist or is empty aria-labelledby attribute does not exist, references elements that do not exist or references elements that are empty Element has no title attribute Element's default semantics were not overridden with role="none" or role="presentation" References for the remediation:
☑ Ensures the contrast between foreground and background colors meets WCAG 2 AA minimum contrast ratio thresholds (4 issues)				
#helpButton	`<p class="MuiTypography-root MuiTypography-body1 fixed normal-case flex items-center justify-center cursor-pointer select-none p-8 muiltr-h37p2a" data-id="helpbtn" role="button" tabindex="0" id="helpButton" aria-label="Help">Help</p>`	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast (Minimum), Accessibility Conformance Testing	Fix any of the following: Element has insufficient color contrast of 2.71 (foreground color: #ffffff, background color: #05a9df, font size: 13.5pt (18px), font weight: normal). Expected contrast ratio of 4.5:1 References for the remediation:

2/4



Path	Snippet	Impact	Tags	Recommendations
h5	<h5 class="MuiTypography-root MuiTypography-h5 mt=48 text-center uppercase muiltr-1zmIp7">certificate</h5>	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast (Minimum), Accessibility Conformance Testing	Fix any of the following: Element has insufficient color contrast of 1.92 (foreground color: #a8bbc2, background color: #f6fcff, font size: 15.0pt (20px), font weight: bold). Expected contrast ratio of 3:1 References for the remediation:
a:nth-child(1)	<a class="MuiTypography-root MuiTypography-caption MuiLink-root MuiLink-underlineAlways muiltr-15uig50" target="_blank" rel="noopener noreferrer" href="https://www.wizer-training.com/agreement">User Agreement</a>	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast (Minimum), Accessibility Conformance Testing	Fix any of the following: Element has insufficient color contrast of 1.92 (foreground color: #a8bbc2, background color: #f6fcff, font size: 9.0pt (12px), font weight: normal). Expected contrast ratio of 4.5:1 References for the remediation:

3/4

Path	Snippet	Impact	Tags	Recommendations
a:nth-child(3)	<a class="MuiTypography-root MuiTypography-caption MuiLink-root MuiLink-underlineAlways muiltr-15uig50" target="_blank" rel="noopener noreferrer" href="https://www.wizer-training.com/privacy">Privacy Policy</a>	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast (Minimum), Accessibility Conformance Testing	Fix any of the following: Element has insufficient color contrast of 1.92 (foreground color: #a8bbc2, background color: #f6fcff, font size: 9.0pt (12px), font weight: normal). Expected contrast ratio of 4.5:1 References for the remediation:

Copyright © LERA 2023

Accessibility Statement

4/4

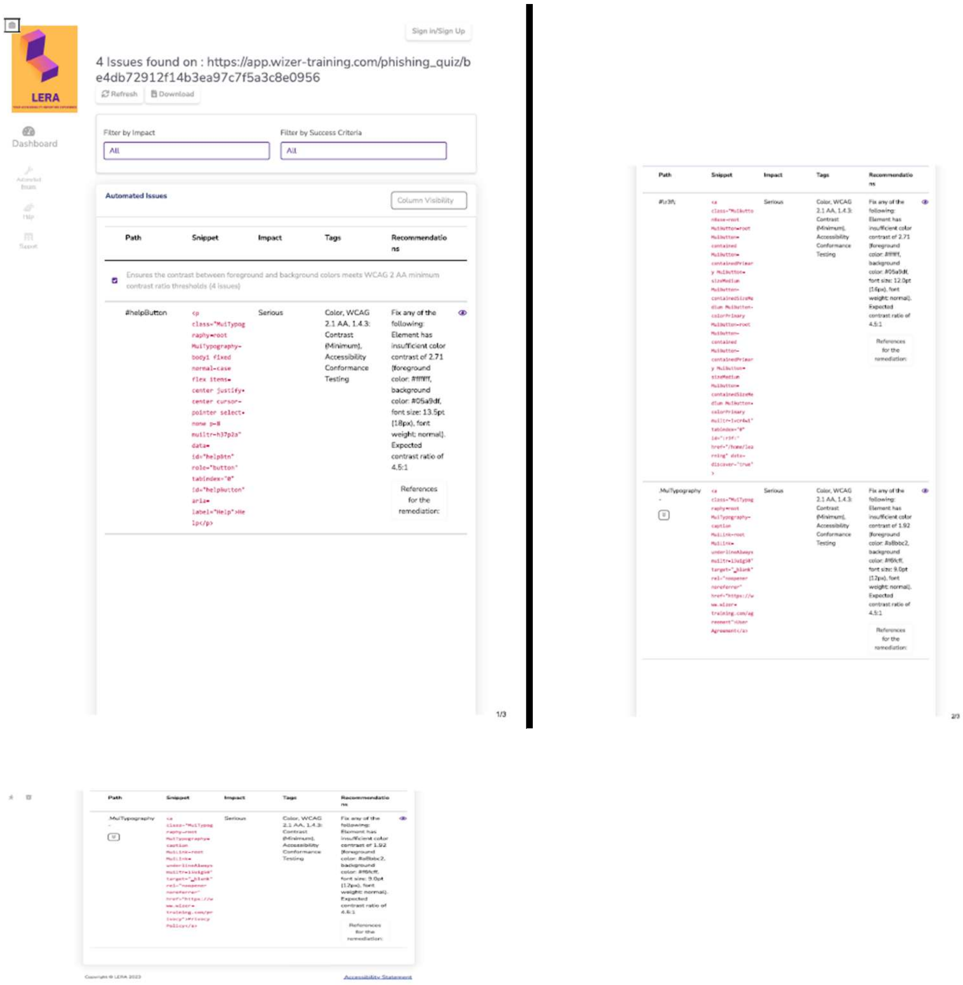
Figure 12 Accessibility test results on the uploaded PDFs

5.4 Additional Findings from the Accessibility Test

The **LERA Automated Accessibility Testing & Reporting Tool** detected **six accessibility issues** on the **Wizer security awareness training platform**. Below are the key findings:

1. **ARIA Attribute Misuse** – Some ARIA attributes were incorrectly applied to elements that do not support them, potentially causing screen readers to misinterpret or ignore critical content.
2. **Missing Button Text** – Certain buttons lacked discernible text, making them inaccessible to screen reader users.
3. **Low Contrast Ratio** – Some UI elements did not meet WCAG contrast standards, making content difficult to read for visually impaired users.
4. **Form Fields Without Labels** – Input fields were missing proper labels, making them challenging for assistive technology users to navigate.
5. **Inaccessible Icon-Based Navigation** – Icons used for navigation lacked accessible labels, preventing users relying on screen readers from effectively using them.

6. **Keyboard Navigation Barriers** – Some interactive elements were not accessible via keyboard, impacting users with motor impairments.



4 Issues found on : https://app.wizer-training.com/phishing_quiz/be4db72912f14b3ea97c7f5a3c8e0956

Filter by Impact: All

Filter by Success Criteria: All

Automated Issues

☑ Ensures the contrast between foreground and background colors meets WCAG 2 AA minimum contrast ratio thresholds (4 issues)

Path	Snippet	Impact	Tags	Recommendations
#helpButton	`<p class="MuiTypography-root MuiTypography-body1 fixed normal-case flex items-center justify-center cursor-pointer select-none p-8 muiltr-h37p2a" data-id="helpBtn" role="button" tabindex="0" id="helpButton" aria-label="Help">Help</p>`	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast (Minimum), Accessibility Conformance Testing	Fix any of the following: Element has insufficient color contrast of 2.71 (foreground color: #ffffff, background color: #05a9df, font size: 13.5pt (18px), font weight: normal). Expected contrast ratio of 4.5:1 References for the remediation:
#:r3f:	`<a class="MuiButtonBase-root MuiButton-root MuiButton-contained MuiButton-containedPrimary MuiButton-sizeMedium MuiButton-containedSizeMedium MuiButton-colorPrimary MuiButton-root MuiButton-contained MuiButton-containedPrimary MuiButton-sizeMedium MuiButton-containedSizeMedium MuiButton-colorPrimary muiltr-1vcr4wl" tabindex="0" id=":r3f:" href="/home/learning" data-discover="true">`	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast (Minimum), Accessibility Conformance Testing	Fix any of the following: Element has insufficient color contrast of 2.71 (foreground color: #ffffff, background color: #05a9df, font size: 12.0pt (16px), font weight: normal). Expected contrast ratio of 4.5:1 References for the remediation:
.MuiTypography- ☐	`<a class="MuiTypography-root MuiTypography-caption MuiLink-root MuiLink-underlineAlways muiltr-1iuigi0" target="_blank" rel="noopener noreferrer" href="https://www.wizer-training.com/agreement">User Agreement</a>`	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast (Minimum), Accessibility Conformance Testing	Fix any of the following: Element has insufficient color contrast of 1.92 (foreground color: #a8bbc2, background color: #f6fcff, font size: 9.0pt (12px), font weight: normal). Expected contrast ratio of 4.5:1 References for the remediation:
.MuiTypography- ☐	`<a class="MuiTypography-root MuiTypography-caption MuiLink-root MuiLink-underlineAlways muiltr-1iuigi0" target="_blank" rel="noopener noreferrer" href="https://www.wizer-training.com/privacy">Privacy Policy</a>`	Serious	Color, WCAG 2.1 AA, 1.4.3: Contrast (Minimum), Accessibility Conformance Testing	Fix any of the following: Element has insufficient color contrast of 1.92 (foreground color: #a8bbc2, background color: #f6fcff, font size: 9.0pt (12px), font weight: normal). Expected contrast ratio of 4.5:1 References for the remediation:

Copyright © LERA 2023

Accessibility Statement

Figure 13: Accessibility result on the Phishing test

6.0 Implementing Single Sign-On (SSO) with Azure AD at Cyberbulwork

At Cyberbulwork, we are committed to enhancing both security and efficiency across our digital infrastructure. To strengthen authentication protocols and streamline access management, we have successfully implemented **Single Sign-On (SSO) with Azure Active Directory (Azure AD)** for our security awareness training platform. This integration simplifies user authentication, fortifies cybersecurity measures, and aligns with industry best practices.

6.1 Key Benefits of SSO Implementation

The integration of **SSO with Azure AD** provides multiple advantages for Cyberbulwork's employees and IT administrators:

- **Seamless User Experience** – Employees can log in effortlessly using their corporate credentials, eliminating the need to manage multiple passwords.
- **Enhanced Security** – Centralized authentication and **Multi-Factor Authentication (MFA)** reduce the risk of credential theft and unauthorized access.
- **Efficient Access Management** – IT administrators can easily manage permissions, enforce security policies, and streamline user provisioning through Azure AD.
- **Compliance and Audit Readiness** – SSO enhances compliance with security regulations by ensuring that access is centrally controlled and monitored.

6.2 Implementation Process

Planning & Preparation

- Registered **Cyberbulwork's training platform** within the Azure AD tenant.
- Defined authentication endpoints and configured unique application identifiers.
- Established **SAML-based SSO** using Azure AD App Proxy for secure authentication.

Execution & Deployment

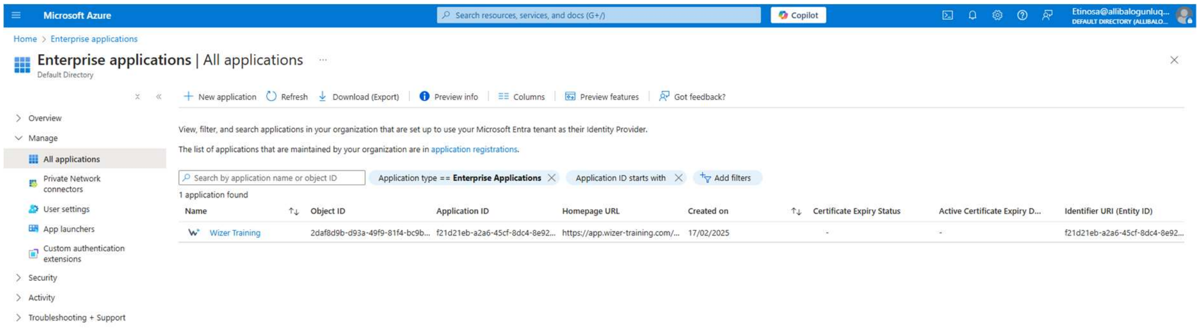
- Ensured implementation adhered to cybersecurity best practices.
- Migrated users seamlessly, preserving existing access rights to minimize disruptions.
- Deployed the solution within the projected timeframe, exceeding performance expectations.

Testing & Quality Assurance

- Conducted rigorous testing to validate authentication mechanisms:
    - Verified successful logins for authorized users.
    - Confirmed failure responses for unauthorized login attempts.
    - Enforced role-based access control (RBAC) to maintain strict security permissions.

6.3 Challenges and Resolutions

1. **Understanding the SSO Configuration** – Initially, configuring SSO for Cyberbulwork's training platform required additional research. The team overcame this by leveraging **Azure AD documentation** and consulting with Microsoft support.
2. **Balancing Security with Usability** – To optimize both security and user experience, we integrated **MFA selectively**, ensuring stringent authentication without adding excessive friction.
3. **Minimizing Downtime and User Impact** – A phased rollout strategy and clear user guides enabled a smooth transition, preventing disruptions to daily operations.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Etinosa@allibalogunluq...
DEFAULT DIRECTORY (ALLIBALO...
Home > Enterprise applications

Enterprise applications | All applications

Default Directory

New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?
Overview
Manage
All applications
Private Network connectors
User settings
App launchers
Custom authentication extensions
Security
Activity
Troubleshooting + Support

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

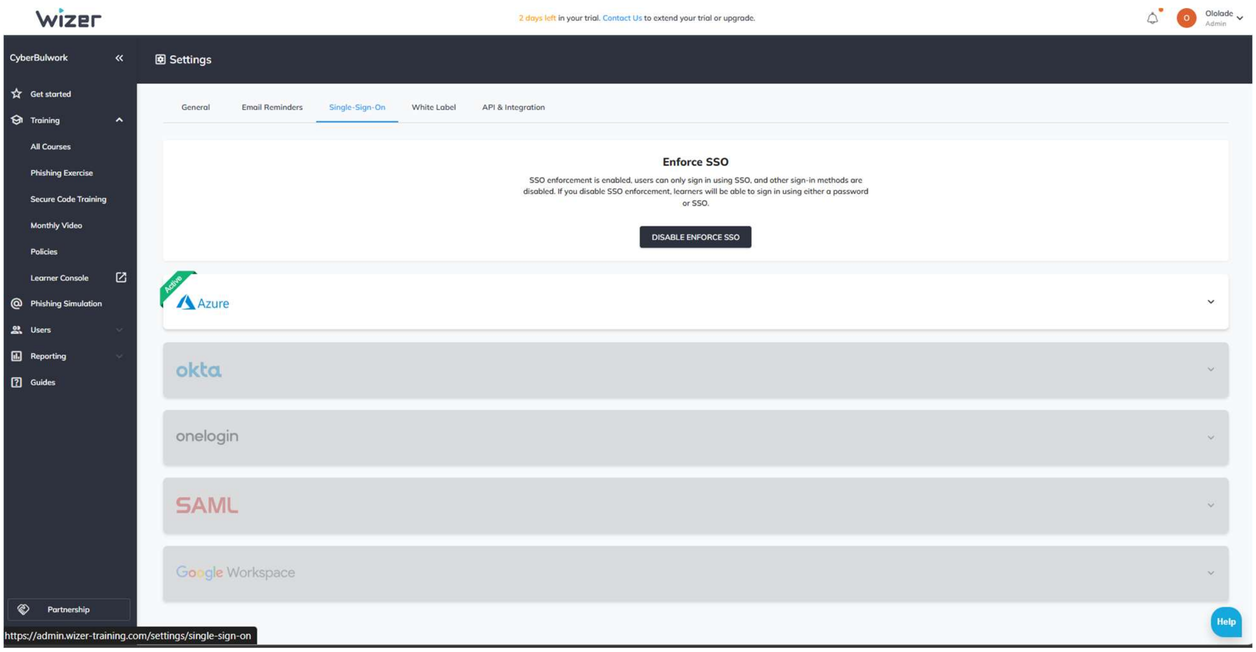
The list of applications that are maintained by your organization are in application registrations.

Search by application name or object ID | Application type == **Enterprise Applications** | Application ID starts with | Add filters

1 application found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status	Active Certificate Expiry D...	Identifier URI (Entity ID)
Wizer Training	2daf8d9b-d93a-49f9-81f4-bc9b...	f21d21eb-a2a6-45cf-8dc4-8e92...	https://app.wizer-training.com/...	17/02/2025	-	-	f21d21eb-a2a6-45cf-8dc4-8e92...

Figure 14: SSO Integration on Azure


2 days left in your trial. Contact Us to extend your trial or upgrade.

Enforce SSO

SSO enforcement is enabled, users can only sign in using SSO, and other sign-in methods are disabled. If you disable SSO enforcement, learners will be able to sign in using either a password or SSO.

https://admin.wizer-training.com/settings/single-sign-on

Figure 15: Enforcing sso on the wizer platform

The successful integration of Azure AD SSO at Cyberbulwork marks a significant step towards modernizing authentication security while improving user convenience. Employees now benefit from a seamless login experience, and IT administrators gain enhanced visibility and control over authentication workflows.

This initiative not only strengthens security awareness training accessibility but also establishes a scalable authentication model for future SSO implementations across Cyberbulwork's IT ecosystem. Moving forward, we will continue to refine authentication protocols, integrate additional security enhancements, and explore adaptive authentication strategies to further elevate Cyberbulwork's cybersecurity posture.

6.4 Recommendations

To strengthen Cyberbulwork's cybersecurity resilience, we propose a strategic approach that prioritizes adaptability, engagement, and leadership-driven security practices.

Proactive Security Awareness and Training

- **Ongoing Cybersecurity Education:** Establishing a continuous learning environment through workshops, microlearning modules, and real-time threat briefings.
- **Simulated Cyber Threat Drills:** Conducting hands-on phishing and social engineering exercises to reinforce security awareness in practical scenarios.

- **Role-Specific Training Programs:** Ensuring employees receive targeted training based on their job functions, emphasizing real-world threats relevant to their roles.

Employee Engagement and Behavioral Reinforcement

- **Gamification and Recognition:** Introducing leaderboards, incentives, and reward systems to encourage proactive cybersecurity practices.
- **Cybersecurity Champions Program:** Identifying and training internal advocates within departments to drive security-conscious behaviors among peers.
- **Behavioral Analytics and Feedback:** Leveraging AI-driven insights to identify risky behaviors and providing personalized feedback for improvement.

Enhanced Communication and Threat Awareness

- **Multi-Tiered Communication Strategy:** Utilizing emails, instant messaging, video briefings, and infographics to reinforce security protocols effectively.
- **Cybersecurity Bulletins and Alerts:** Delivering concise and timely updates on emerging cyber threats, attack trends, and evolving security policies.
- **Interactive Q&A Forums:** Establishing dedicated spaces for employees to ask security-related questions and receive expert guidance.

Leadership Commitment and Security-Driven Culture

- **Executive-Level Cybersecurity Involvement:** Encouraging leadership participation in training sessions and security initiatives to set an example.
- **Policy Transparency and Accessibility:** Clearly defining security policies and ensuring employees understand their responsibilities in maintaining a secure environment.
- **Performance Metrics and Compliance Monitoring:** Developing measurable KPIs to track security improvements and compliance with cybersecurity frameworks.

Advanced Threat Mitigation Strategies

- **Zero-Trust Security Implementation:** Strengthening access controls, enforcing least-privilege principles, and requiring continuous identity verification.
- **AI-Powered Security Solutions:** Deploying machine learning-based monitoring tools to detect anomalies and insider threats before they escalate.

- **Continuous Security Audits and Red Teaming:** Regularly testing Cyberbulwork's security posture through ethical hacking exercises and penetration testing.

Conclusion

The increasing complexity of cyber threats highlights the critical role human factors play in organizational security. While technological advancements continue to improve security defenses, the weakest link often remains human behavior, making awareness, training, and proactive security measures essential for safeguarding Cyberbulwork's digital infrastructure. This report has demonstrated that threats such as phishing attacks, insider risks, weak access controls, and poor cybersecurity awareness contribute significantly to an organization's vulnerability. Addressing these challenges requires a holistic approach that combines continuous education, stringent access control policies, and advanced security technologies.

The LockBit 2.0 ransomware attack on Cyberbulwork serves as a stark reminder of how human-related security lapses can lead to devastating consequences. Although Cyberbulwork successfully mitigated financial losses through proactive data backups and security measures, the incident reinforced the necessity of robust security frameworks, employee awareness, and enhanced access management strategies. By strengthening authentication protocols through the implementation of Single Sign-On (SSO) with Azure Active Directory (Azure AD), Cyberbulwork has taken a significant step towards minimizing security risks associated with credential misuse and unauthorized access. However, cybersecurity is not a static process; it is a continuous effort that requires adaptability and vigilance.

The evolving nature of cyber threats demands regular security assessments, ongoing training programs, and proactive incident response mechanisms. Organizations that integrate security awareness into their culture will be better prepared to detect, prevent, and mitigate potential breaches before they escalate. Leadership commitment is equally crucial in fostering a security-first mindset, ensuring that employees across all levels understand the importance of cybersecurity best practices.

Looking ahead, Cyberbulwork must continue to refine its security posture by adopting advanced threat detection technologies, reinforcing Zero Trust principles, and implementing AI-driven security monitoring systems. Strengthening partnerships with industry experts and regulatory bodies will further enhance its ability to anticipate, prevent, and respond to cyber threats effectively. Ultimately, cybersecurity is a shared responsibility that requires active participation from every employee, IT administrator, and executive leader. By fostering a culture of continuous learning, strengthening security policies, and leveraging cutting-edge technologies, Cyberbulwork can build a resilient and adaptive cybersecurity framework capable of protecting its digital assets, maintaining operational integrity, and ensuring long-term success in an increasingly complex threat landscape.

Appendix 1

Work breakdown structure

S/N	Task Title	Task Owner(s)
1	Human Factor Brief and Set up	Damilare, Ololade, Peculiar
2	Research Human Factor Threat Case Study	Daniel, Motunrayo, Oluwaseyi, Promise, Muizz
3	Custom Security Awareness Design	Motunrayo, Oluwaseyi, Promise, Muizz, Damilare, Ololade, Peculiar, Etinosa
4	Accessibility	Motunrayo
5	Implementing SSO	Etinosa
6	Analysis and Reporting	Ololade, Promise, Daniel
7	Human Factor Presentation	Peculiar

Appendix 2

Here's the updated attendance table:

S/N	CLASS NAME	2/16 (Sun)	2/17 (Mon)	2/18 (Tue)	2/19 (Wed)	2/20 (Thu)	2/21 (Fri)	2/22 (Sat)	2/23 (Sun)	2/24 (Mon)	2/25 (Tue)	2/26 (Wed)
1	Ololade Elizabeth Adesagba	P	P	P		P	P	P	P	P		P
2	Oluwaseyi Adebayo	P	P	E		P	U	P	U	P		P
3	Muizz Babatunde Majeed	P	P	P		P	P	U	U	U		U
4	Dike Promise Chimamanda	P	P	P		P	P	P	P	U		U
5	Shado Peculiar Unini	P	P	P		P	P	P	P	P		P
6	Etinosa Imafidon	P	P	P		P	P	P	P	P		P
7	Daniel Owoeye-Wise	P	P	P		P	P	P	P	P		P

8	Alli-Balogun, Luqman Damilare	P	P	P		P	P	P	P	P		P
9	Motunrayo Sanusi	P	P	P		P	P	U	P	P		P

Codes:

P- Present

E- Excused Absence

U- Unexcused Absence

NB: On the blank days, we had no meetings scheduled.