OHIO AUDITOR OF STATE
KEITH FABER

65 East State Street
Columbus, Ohio 43215
ContactUs@ohioauditor.gov
800-282-0370

Auditor of State Advisory Memo

To: **All Auditor of State Clients**

From: **Keith Faber, Auditor of State**

Date: **July 15, 2026**

Subject: **Best Practice: Importance of Multi-Factor Authentication (MFA) and Risks of Unauthorized Access to Internal Portals**

In 2025, the Auditor of State released Bulletin 2025-007 detailing the cybersecurity requirements as outlined in Ohio Rev. Code Section 9.64, which includes developing safeguards against cybersecurity threats. As part of our ongoing cybersecurity observations and risk assessments, we continue to see a growing number of incidents involving compromised accounts that subsequently lead to unauthorized access to internal systems, payroll platforms, vendor management portals, and other business applications. These attacks are not limited to highly privileged accounts; any user account can be a target. The compromise of even a basic user account can provide an opening for malicious activity.

A common attack scenario begins when a threat actor gains access to a user's account through phishing, credential theft, password reuse, or other means. Once inside the account, the attacker is often able to use password reset functionality to gain access to additional systems that rely solely on email-based account recovery. This frequently enables unauthorized access to internal forms, workflows, and administrative functions that can be used to redirect payroll deposits, alter vendor banking information, initiate fraudulent payments, or compromise sensitive company data. Proper use of MFA can help reduce the risk of these types of attacks.

What Is MFA?

MFA is a security control that requires users to provide two or more forms of verification before gaining access to a system or application.

Typically, MFA combines:

- Something you know (password or PIN)
- Something you have (authentication application, security token, or mobile device)

- Something you are (biometric authentication such as a fingerprint or facial recognition)

By requiring multiple forms of authentication, MFA significantly reduces the likelihood that a compromised password alone can be used to gain unauthorized access.

Why MFA Matters

Many organizations continue to rely on passwords as the primary means of authentication. However, passwords are routinely compromised through phishing campaigns, malware, social engineering, and data breaches.

Without MFA, a stolen password may provide an attacker with immediate access to accounts, cloud applications, payroll systems, vendor portals, and other critical business functions.

Even when an application is not directly compromised, access to an employee's email account can allow an attacker to reset passwords for other systems, effectively bypassing the intended security of those applications.

MFA serves as a critical secondary control that can prevent unauthorized access even when user credentials have been compromised.

Alignment with Recognized Security Frameworks

The implementation of MFA is consistently recommended by leading cybersecurity frameworks and standards, including:

- National Institute of Standards and Technology (NIST) cybersecurity guidance, including the Cybersecurity Framework (CSF) and Digital Identity Guidelines
- Center for Internet Security (CIS) Critical Security Controls
- Cybersecurity and Infrastructure Security Agency (CISA) guidance on phishing and business email compromise prevention

These frameworks consistently identify MFA as one of the most effective controls available for reducing the risk of unauthorized system access.

Key Recommendations

1. Implement MFA Across All Systems

Organizations should require MFA for:

- Email systems
- Cloud applications

- Payroll platforms
- Vendor management portals
- Remote access solutions
- Virtual private networks (VPNs)
- Administrative accounts
- Any internet-facing application containing sensitive information or functionality

MFA should be enforced consistently across the organization with **no exceptions**, including executive leadership, senior management, board members, system administrators, and other privileged users.

Threat actors frequently target executives because of their elevated access, authority, and ability to approve financial transactions. Excluding executive users from MFA requirements creates a significant security vulnerability.

2. Apply MFA Requirements to Vendors and Third Parties

Organizations should ensure that vendors, contractors, consultants, managed service providers, and other third-party users are subject to the same MFA requirements as employees.

Third-party access often represents a significant attack surface and should be governed by the same security standards applied to internal users. An organization's security posture is only as strong as the weakest access point connected to its systems.

MFA alone is not sufficient. The following recommendations, combined with well executed MFA, strengthen overall security and reduce an entity’s overall threat exposure.

3. Limit Exposure of Internet-Facing Portals

Organizations should carefully evaluate what information, forms, procedures, workflows, and administrative functions are accessible through internet-facing portals.

Sensitive resources such as:

- Payroll change requests
- Direct deposit modification forms
- Vendor banking update forms
- Payment authorization workflows
- Human resources records

- Administrative procedures and internal process documentation should not be accessible through publicly exposed portals without strong authentication controls.

Where practical, organizations should restrict access to sensitive functions through MFA-protected environments and apply role-based access controls that limit users to only the information and functionality required for their job responsibilities.

4. Strengthen Password Reset and Account Recovery Controls

Many recent fraud incidents have originated from weak account recovery processes.

Organizations should review password reset procedures to ensure they do not rely solely on email access as proof of identity. If a user's email account becomes compromised, an attacker should not be able to use that access to gain control of additional systems.

Password reset and account recovery processes should incorporate additional verification measures such as:

- MFA verification
- Identity validation procedures
- Administrative review and approval for high-risk account changes
- Alerts and monitoring for account recovery events

5. Monitor High-Risk Changes

Organizations should implement additional controls around changes involving:

- Vendor banking information
- Payroll direct deposit information
- Payment instructions
- User access privileges

High-risk changes should require independent verification, approval workflows, and monitoring to detect unauthorized activity.

Conclusion

The increasing frequency of account compromise incidents demonstrates that password-only security is no longer sufficient to protect business-critical systems and processes.

Organizations should operate under the assumption that user credentials may eventually be compromised and implement layered security controls designed to prevent a single compromised account from resulting in broader system access or financial fraud.

At a minimum, organizations should implement MFA for all users and third parties without exception, strengthen password reset controls, and carefully evaluate what information and functionality are exposed through internet-facing portals. These measures align with leading cybersecurity frameworks such as NIST and CIS and can significantly reduce the risk of payroll diversion schemes, vendor payment fraud, unauthorized access, and other cyber-related financial losses.

Please review your current practices and consider implementing or updating your policy accordingly.

Thank you for your attention to this matter. If you have any questions, please contact your regional AOS office using Contact Us (https://ohioauditor.gov/contact.html) on the AOS website.