



Cyber Spotlight

A quarterly insight from Optima's Cybersecurity team

OCTOBER 2026

Cybersecurity Awareness Month

October is Cybersecurity Awareness Month! At Optima, we would like to highlight some practical cybersecurity best practices that can help your organization strengthen its defenses against scams, phishing, and account breaches.

Why MFA Matters

Multi-factor authentication (MFA) is an effective security control that requires users to provide two or more distinct verification factors before accessing accounts and systems.

These verification methods generally fall into three categories: something you know, something you have, or something you are. In other words, MFA may combine something you know, like a password, with something you have, like a smartphone authenticator app, or something you are, like a fingerprint.

Common MFA methods include text or email codes, authenticator apps, security keys, and device-based biometrics such as Face ID. Even if an attacker obtains a password, MFA adds another barrier to unauthorized access. Cybersecurity authorities, including CISA and NIST, recommend enabling MFA wherever it is available, with particular attention to sensitive and privileged accounts. This establishes an additional layer of security to help protect your organization and can provide significant security benefits with relatively little impact on day-to-day operations.

Why Some Forms of MFA Can Be Bypassed

Although MFA is a strong and versatile security control, there are ways for attackers to bypass it. Historically, malicious actors have used open-source adversary-in-the-middle (AiTM) frameworks, such as Evilginx, to bypass MFA controls. In June 2026, **CloudSEK discovered BigBear 2.0**, a re-branded Evilginx2-based phishing-as-a-service (PhaaS) framework. An Evilginx-based phishing attack may begin with a convincing email that links

to a counterfeit sign-in page designed to resemble a legitimate service. When a user enters credentials and completes an MFA prompt, the attacker's proxy relays the authentication to the legitimate service in real time. After authentication, the attacker can capture the resulting session cookie. By replaying that cookie, the attacker may hijack the authenticated session without completing another MFA challenge.

Evilginx2 expands on the original framework with improved capabilities for configuring and managing phishing campaigns. Its tooling simplifies the creation and management of phishing templates that impersonate sign-in pages for specific services.

According to CloudSEK, the BigBear 2.0 campaign targeted hundreds of organizations across more than 40 countries, resulting in thousands of stolen credentials and session cookies, demonstrating the potential scale of modern phishing attacks.

How AI Is Changing Phishing

While artificial intelligence (AI) has been widely adopted to automate repetitive tasks and improve workplace efficiency, malicious actors have begun using similar tools in their attacks.

By utilizing AI to generate text, traditional warning signs, such as poor grammar and spelling, may be less obvious. AI can also help attackers gather and analyze publicly accessible information about an organization and use it to create more convincing, personalized phishing messages.

Real names, departments, or other organization-specific information found on LinkedIn or other networks can be used to make phishing campaigns appear more credible.

AI has also significantly reduced the time and effort required to develop these campaigns. Research, drafting, and personalization that previously would have required substantial manual effort can now be completed much faster, enabling malicious actors to create targeted phishing campaigns at a larger scale.

How to Improve Security with Phishing-Resistant MFA

As technology evolves, attackers continue to develop methods for bypassing security controls. A single layer of security, such as antivirus software, is rarely enough to protect an organization.

Defense in depth is a security approach that combines different layers of security measures to protect an organization's assets.

Phishing-resistant MFA is one preventive control that helps defend against common MFA-bypass techniques. It uses public-key cryptography to verify both the user and the legitimate service. The user's device holds a private key, while the service stores the corresponding public key. During sign-in, the device signs a challenge that is bound to the legitimate website, and the service verifies the response. Because the private key never leaves the device and the response is tied to the legitimate domain, a counterfeit site cannot reuse it to authenticate. Implementing phishing-resistant MFA can help protect an organization's sensitive accounts even when an employee falls victim to phishing. Combined with effective cybersecurity training and recurring simulated phishing exercises, it can strengthen an organization's defenses against phishing and social engineering, which remain common and persistent cyber threats.

Why Regular Security Assessments Matter

Cybersecurity frameworks such as the NIST Cybersecurity Framework emphasize regular risk assessments as part of an ongoing risk-management program. A security assessment evaluates relevant areas of an organization's environment, including its external attack surface, network security, technical controls, and policies. A comprehensive assessment provides a top-down view of the organization's strengths, identifies areas for improvement, and offers practical recommendations.

How Optima Can Help

Optima Partners offers security assessments as part of our broader cybersecurity services. We also provide vulnerability management, penetration testing, vendor risk management, tabletop exercises, policy development and management, cybersecurity training, and phishing simulations.

Prepare Your Firm for Responsible AI Use

Optima Partners offers AI Readiness Assessments and AI Staff Training to help firms understand how AI is currently being used, identify potential risks and governance gaps, and establish practical safeguards for employees. Whether your firm is just beginning to explore AI or already using it across the organization, our team can help you develop a responsible and informed approach.

To learn more, contact
cyber-sales@optima-partners.com.