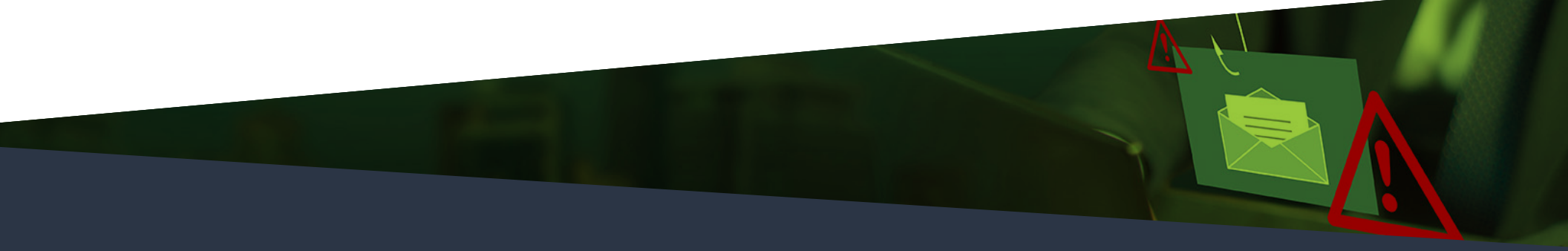

Prepared for

yubico

The Evolving Threat of Phishing and Social Engineering

August 2024 EMA White Paper

By **Christopher M. Steffen, CISSP, CISA, CCZT**, VP of Research
Information Security, Risk, and Compliance Management

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Despite ongoing advancements in security technologies and processes, it continues to be fairly simple to compromise user credentials through phishing and social engineering attacks, and we are seeing this become even easier with the advancements of AI, deepfakes and voice cloning. Plenty of examples exist and are exploited daily: social media is a literal warehouse of personal information that bad actors can use to target help desks, answer security questions, and ultimately resetting passwords. This allows them to enroll new devices to which multifactor authentication (MFA) codes are sent. From there, they can easily bypass MFA and gain access to any/all resources in an environment.

This is just one example that illustrates the limitations of basic authentication methods like passwords, OTP and SMS-based MFA, which social engineering tactics can easily defeat. Social media underscores the urgent need for a new, modern phishing-resistant approach to authentication and user security.

Phishing-Resistant Users: The Next Evolution

There are solutions in the market that are resistant to phishing attacks. Cultivating and educating people to become phishing-resistant users ensures that their entire credential lifecycle – from onboarding to authentication to account recovery – is resistant to phishing and social engineering attacks.

These solutions require a shift away from credentials and processes that can be easily compromised, like passwords, codes and knowledge-based security questions. Instead, the focus should be on authentication methods that are inherently resistant to phishing, such as hardware security keys (like YubiKeys).

Classifying Passkey Credentials

There are three major types of passkeys (FIDO2 credentials) that can be found in the market today:

- **Synced passkeys.** These are copyable credentials that can be used across multiple devices. While convenient, they offer lower security assurance.
- **Device-bound passkeys on general-purpose devices.** These reside on smartphones, tablets, and other everyday devices. They provide a middle-ground option for enterprises, but still have security limitations compared to hardware security keys.
- **Device-bound passkeys on purpose-built security devices.** These are passkeys stored on specialized hardware security devices, like YubiKeys. This category offers the highest level of security and compliance assurance (meeting the AAL3 standard), making it the optimal choice for enterprises.

It is important to note that not all device-bound passkeys are created equal. Passkeys stored on general-purpose devices, while an improvement over traditional credentials, still carry inherent risks due to their copyable/sharable nature and lower security/compliance assurance. In contrast, passkeys on purpose-built security keys provide the highest level of phishing resistance and meet the strictest security standards, while providing several operational benefits.

The Benefits of Phishing-Resistant Users

There are benefits to creating "phishing-resistant users" through the use of purpose-built security devices:

- **Enhanced cybersecurity resilience.** By eliminating phishing vulnerabilities across the entire user credential lifecycle, enterprises can significantly reduce their risk exposure and improve overall security posture.

- **Improved operational efficiency.** Streamlined onboarding, authentication, and credential recovery processes can reduce help desk calls, user training requirements, reduced user downtime and other operational overhead.
- **Protecting the entire user credential lifecycle.** Securing the entire lifecycle, from initial registration to ongoing authentication and recovery, ensures that phishing resistance is maintained at all points of user interaction.
- **Ensuring safe access from anywhere.** Phishing-resistant authentication methods enable secure access for remote and mobile users, regardless of device or location.

By transitioning from "phishing-resistant authentication" to "phishing-resistant users," enterprises can achieve a new level of cybersecurity resilience and operational efficiency while better protecting their users, data, and assets from the growing threat of phishing and social engineering attacks.

Conclusion

Mature security organizations understand the importance of moving beyond just phishing resistant authentication toward the creation of "phishing-resistant users." By securing the entire user credential lifecycle through the use of purpose-built security devices, organizations can significantly enhance their cybersecurity resilience, improve operational efficiency, and better protect their users, data and assets from the growing threat of phishing and social engineering attacks.

EMA Perspective

As analysts, we constantly evaluate the latest trends and technological advances. Some of them are little more than marketing hype, but some eventually become the standard for the industry. Phishing-resistant users will become the standard.

- **Phishing attacks are increasing and becoming more sophisticated:** The bad guys are not trying to hack away at your front door any longer (besides, the "front door" of the enterprise is all but gone at this point). They are looking for better and easier ways to gain entry to your critical systems, and among the easiest to hijack are the credentials of an existing employee. Sophisticated phishing attacks target the users, stealing their credentials to infiltrate systems and compromising sensitive data – a harsh reality many organizations face today. Antiquated controls and processes are designed around protecting devices and systems, not users.
- **Organizations are looking for a better way to MFA:** Organizations rely on MFA, and there are plenty of reasons why. There are regulatory controls, best practice considerations, cyber insurance requirements and simplified user experiences. Users (and security leaders) do not want to increase security friction with their users. They are often burdened with long, complex passwords or outdated methods, like SMS, which are vulnerable and annoying. Even phishing-resistant MFA solutions like passkeys fall short when backed by weak passwords, causing enterprises to swing between security and vulnerability during key stages like onboarding, authentication, and recovery.
- **A phishing-resistant user is the next standard in authentication:** Create phishing-resistant users by employing seamless, secure phishing-resistant authentication across any and all devices, services, and business scenarios. Authentication should start and end with the user, and solutions like Yubikeys are one of the best ways to start down this path.

We – as users, security administrators, even the general public – will always need better methods of authentication to access the environments that we need. Concentrating on the users and not devices is a strong start, and Yubico continues to lead the way.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4448.080624