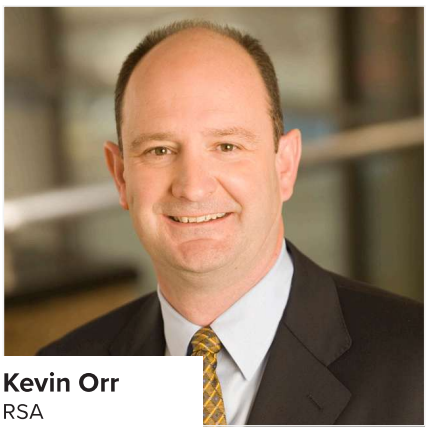
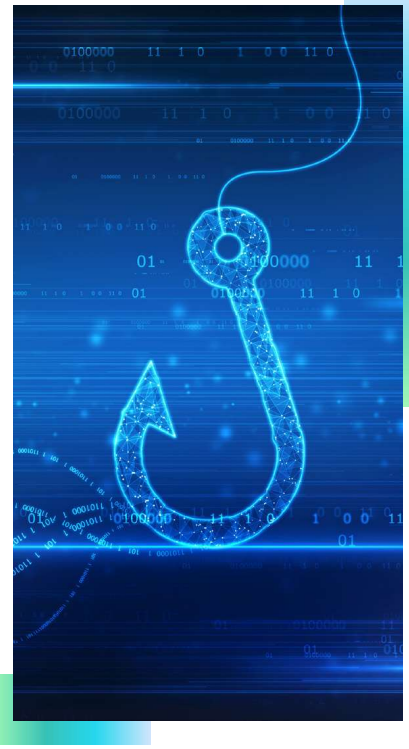
RSA

Undermining phishing by eliminating passwords

Passwordless authentication blocks one of the most successful and damaging attack methods



Kevin Orr
RSA



Phishing is one of the highest-impact and most frequent tactics that cybercriminals use. Such attacks trick users into revealing passwords, usernames and other credentials. According to Verizon's 2025 Data Breach Investigations Report, 22% of breaches began with the use of stolen credentials, and phishing (which leads to stolen credentials) was present in 15% of all breaches. The IBM Cost of a Data Breach Report 2025 found that phishing was one of the most frequent and expensive causes of data breaches, costing an average of $4.8 million and taking an average of 261 days to contain.

IT administrators are wise to assume that hackers are in their networks, but they don't know what data those attackers might be taking or altering. The implications for government are profound. In just one example, what if somebody changed the targeting coordinates for a military operation? That brings a new perspective on the nature of the threat landscape.

Multi-factor authentication (MFA) provides essential cybersecurity capabilities, but today's cyberattacks demand more than traditional MFA to protect networks and resist phishing attempts. They require passwordless authentication.

In a passwordless environment, authentication combines secure possession factors (like tokens or mobile apps) with biometrics, removing the need for vulnerable shared secrets such as passwords.

A complete, organization-spanning solution

To simplify the move to a passwordless environment, RSA provides a complete, enterprise-ready, always-on solution that protects all users in all environments from all threats. Although other vendors cover individual user groups or use cases, RSA delivers organization-spanning passwordless capabilities at scale.

The RSA Authenticator App, offered through RSA ID Plus, supports phishing-resistant device-bound passkeys on iOS and Android devices. Organizations can also deploy RSA's iShield Key 2 series and DS100 FIDO2-certified security keys, featuring upgradable firmware and phishing-resistant authentication.

Furthermore, RSA complements Microsoft environments by strengthening and extending passwordless capabilities in the high-risk and hybrid environments where Microsoft falls short. Microsoft enables strong passwordless access with Windows Hello and FIDO2. RSA extends those capabilities to hybrid, regulated and non-Microsoft environments, helping organizations close any remaining security and operational gaps.

RSA can provide modern passwordless solutions for high-risk roles and for air-gapped, RADIUS and

"IN A PASSWORDLESS ENVIRONMENT, AUTHENTICATION COMBINES SECURE POSSESSION FACTORS (LIKE TOKENS OR MOBILE APPS) WITH BIOMETRICS, REMOVING THE NEED FOR VULNERABLE SHARED SECRETS SUCH AS PASSWORDS."

iOS environments. RSA integrates directly with Microsoft Conditional Access, ensuring organizations can extend Entra's passwordless foundation seamlessly across every environment.

A consistent passwordless log-in experience

There's very little difference between a premeditated cyberattack and a genuine cloud, technology or vendor outage. When the cloud becomes unreachable, organizations that maintain resilient and secure access will thrive while others struggle.

RSA ID Plus Hybrid Failover, the market's only hybrid authentication capability, allows organizations to fall back to on-premises authentication and complete MFA processes using a one-time passcode, even if the cloud is unreachable or if the user's device is in airplane mode.

By extending Microsoft's strong passwordless foundation with federal-grade resilience and coverage from RSA, agencies gain the confidence that mission-critical access will remain secure, compliant and uninterrupted in any scenario. ■

Kevin Orr *is president of RSA Federal.*

ADOBE STOCK // BLACKBOARD