# EINPRESSWIRE

TraitWare Issues Cybersecurity Advisory

Urgent Call for Businesses to Modernize Access Controls Amid Escalating Cyber Threats from Advanced Threat Actors

RENO, NV, UNITED STATES, June 24, 2025 /EINPresswire.com/ -- TraitWare, a leader in phishing-resistant, passwordless multi-factor authentication (MFA) and single sign-on (SSO) for the enterprise, today issued an urgent cybersecurity advisory in response to growing concerns of retaliatory cyber activity

linked to Iranian threat actors. In light of recent geopolitical tensions, organizations are being warned of likely increases in identity-based attacks—leveraged through tactics similar to those used by the well-known Scattered Spider group.
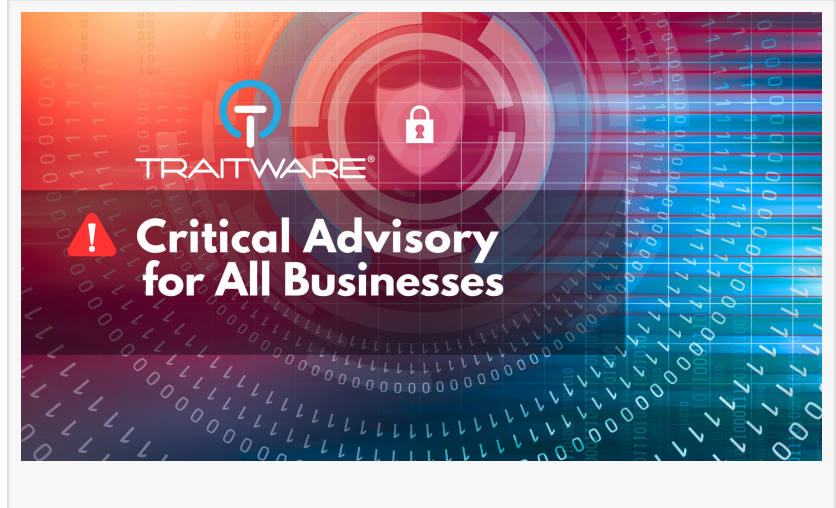
> " These attackers don't break in, they log in. They exploit weaknesses in access controls that most companies still rely on. When you add geopolitical motivation ... the risk compounds dramatically."
>
> *Heath Spencer*

Threat Landscape: Identity Is the Battlefield

Both criminal and nation-state actors have demonstrated increasing sophistication in targeting enterprise identity systems. Groups such as Scattered Spider have breached major corporations through:

- Social engineering of help desks
- MFA fatigue and push notification abuse
- Session hijacking and credential theft

- Abuse of identity providers like Okta and Entra

The group, known as Scattered Spider or UNC3944, initially targeting retail companies, has pivoted to major insurance companies, Google's Threat Intelligence Group (GTIG) said in an email sent to different stakeholders. The group is known for its ability to use social engineering to impersonate employees, deceive IT teams, and bypass multifactor authentication, according to an SOS Intelligence briefing.

"These attackers don't break in—they log in," said Heath Spencer, CEO of TraitWare, Inc. "They exploit weaknesses in access controls that most companies still rely on. And when you add geopolitical motivation to the mix, the risk compounds dramatically."

Phishable vs Phishing-Resistant MFA*

Phishable Factors	Phishing-Resistant Factors
Passwords	Biometrics - Fingerprint, Facial Scan, etc.
Email Push notifications	Cryptographic security keys
SMS messages	Hardware security keys
One-time passcodes (OTPs)	Device-based security checks
Magic Links	Behavior-based authentication
Security questions	

TraitWare Eliminates the Need for Phishable Factors for Login

How Attackers Bypass Traditional MFA

Cybercriminal groups such as Scattered Spider are known for targeting organizations through a blend of social engineering, credential theft, and MFA bypass techniques. In recent alerts, security agencies have highlighted how Scattered Spider operators often start with phishing campaigns to steal employee credentials. Once inside, they attempt to bypass traditional MFA protections—such as SMS-based one-time passwords or push notifications—using tactics like push bombing (spamming victims with MFA requests until one is approved) or intercepting authentication codes through SIM swapping. These methods allow attackers to gain access even when organizations have deployed standard MFA solutions.

Phishing-Resistant MFA: Critical Defense for Identity Systems

The rise in Scattered Spider activity underscores the limitations of traditional MFA, which can be defeated by determined adversaries. In response, security experts are increasingly recommending the adoption of phishing-resistant MFA—such as FIDO2-compliant security keys and/or biometric authentication—which cannot be intercepted or replayed. By requiring physical tokens or unique biometrics that are cryptographically bound to the authenticating site, phishing-resistant MFA effectively blocks the techniques used by groups like Scattered Spider, making it much harder for attackers to gain unauthorized access even if they possess stolen credentials. This shift is essential for organizations seeking to protect themselves against advanced, socially engineered cyberattacks in the current threat landscape.

CISA Guidance Echoed

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) continues to urge organizations to implement phishing-resistant multi-factor authentication (MFA). In the current threat climate—especially with warnings of Iran-backed retaliation cyber ops—the need to move beyond passwords, push codes, and SMS-based MFA has never been more urgent.

A Proven Solution: Passwordless, Phishing-Resistant MFA

TraitWare's patented platform delivers:

- FIDO2-compliant, passwordless login
- Biometric and device-bound identity proofing
- Fast and user-friendly deployment and use across apps, SSO platforms, and endpoint login (Windows/macOS)
- Compliance alignment with NIST, CISA, and Zero-Trust principles

Call to Action

TraitWare urges all organizations, especially those in critical infrastructure, healthcare, financial services, and public sector, to immediately assess their authentication stack.

"Phishing-resistant MFA isn't a future ideal—it's a present necessity," added Spencer. "Waiting is no longer a viable strategy."

About TraitWare

TraitWare is redefining secure access for the enterprise with a patented, phishing-resistant passwordless MFA+SSO solution designed to eliminate shared secrets and stop credential-based attacks before they begin. TraitWare is built with Zero Trust architecture and simplicity at the core, delivering strong authentication from the first point of contact.

Visit us at www.traitware.com for a free trial, or contact us for more information.

Elizabeth Perry
TraitWare
+1 775-710-3999
contact@traitware.com
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.