

CYBERJA

CYBERSECURITY & GRC MAGAZINE

ISSUE 03 | SEPTEMBER 29, 2026

COVER STORY

MFA IS NOT THE FINISH LINE

EvilTokens demonstrates why modern IAM must govern authentication flows, tokens, sessions, devices and post-authentication authority - not just passwords and MFA.

INSIDE

- EvilTokens & device-code phishing
- AI-powered post-compromise reconnaissance
- Token and session governance
- ENISA Threat Landscape 2026
- Supply-chain identity risk
- Ransomware behavior over branding
- AI changing cybercrime economics
- Authentication Flow & Token Assessment
- CyberJA workshop and practical skill paths

From the Editor

MFA remains essential, but this week's developments show why IAM maturity cannot stop at the authentication event. Attackers increasingly abuse legitimate workflows, steal usable tokens, establish persistent sessions, and then use AI to understand the victim's organization at speed.

This issue translates those developments into practical IAM, Zero Trust, cloud-risk and GRC controls you can assess, teach and apply. CyberJA learning paths are integrated throughout so readers can move from insight to practical skill.

CYBERJA PRACTICAL LEARNING

Learn the concept. Practice the assessment. Apply the control.

CyberJA focuses on on-the-job capabilities that add measurable value to cybersecurity and GRC work.

[Explore CyberJA Resources ->](#)

Executive Outlook: Authentication Assurance Is Not Enough

Microsoft's disruption of EvilTokens provides a large-scale example of device-code phishing, token theft, cloud reconnaissance, AI-assisted mailbox analysis and fraud preparation. ENISA's 2026 threat landscape simultaneously reinforces ransomware, vulnerability exploitation, dependencies, supply-chain risk and growing AI enablement.

CORE MESSAGE

Move from MFA thinking to continuous identity assurance

Govern how authentication occurs, what token and session result from it, which device is involved, what authority is exercised, and whether behavior remains trustworthy.

1 | EvilTokens: MFA Can Succeed While the Attack Succeeds

Microsoft disclosed and disrupted EvilTokens, a phishing-as-a-service platform that used device-code phishing to manipulate legitimate authentication. A victim could complete the real Microsoft flow - including password and MFA - while unknowingly authorizing the attacker's session.

Why it matters for IAM governance

The lesson is not that MFA is ineffective. The lesson is that MFA validates an authentication step, not the entire transaction. IAM programs should govern the authentication flow itself and tightly restrict flows that are unnecessary.

Assessment question	Evidence
Is device-code authentication enabled?	Conditional Access / IdP configuration
Which apps genuinely require it?	Application inventory
Which identities can use it?	IAM policy
Are exceptions risk-accepted?	Exception register
Are token anomalies monitored?	SIEM detections
Can sessions be centrally revoked?	IR test evidence

CYBERJA SKILL PATH

Implement effective IAM governance

Build practical capability in identity lifecycle, least privilege, access reviews, approvals, segregation of duties, privileged access and modern identity assurance.

[Explore Effective IAM Governance ->](#)

[Microsoft Security Blog](#)

2 | AI After Compromise: The Mailbox Becomes Attack Intelligence

The standout AI lesson from EvilTokens is what happens after identity compromise. AI can rapidly analyze a mailbox for trusted relationships, executives, vendors, payment conversations and financial authority. A compromised inbox is therefore not merely a collection of messages; it can become machine-readable organizational intelligence.

INCIDENT RESPONSE

Reassess mailbox compromise impact

Assume attackers can rapidly reconstruct business relationships, payment workflows and authority structures. Containment speed and business-impact analysis should reflect that possibility.

CYBERJA SKILL PATH

Manage AI risk in the business

Learn to identify and manage security, privacy, operational, third-party and business risks created by AI adoption and AI-enabled threats.

[Explore Management of AI Risk ->](#)

3 | Token Theft Makes Session Governance a Core IAM Discipline

Modern identity response cannot end with a password reset. If valid tokens, refresh tokens, registered devices or active sessions remain usable, the attacker may retain access.

IDENTITY CONTAINMENT

Use a complete cloud identity response

Disable/restrict identity; revoke sessions and refresh tokens; reset credentials; review MFA/passkeys; remove unauthorized devices; review OAuth grants, inbox rules, Graph/API activity and cloud-file downloads.

CYBERJA SKILL PATH

Conduct practical cybersecurity assessments

Assess maturity, collect evidence, identify control gaps and convert findings into prioritized business improvements.

[Explore Practical Cybersecurity Assessments ->](#)

4 | ENISA 2026: Dependencies Are Systemic Cyber Risk

ENISA's Threat Landscape 2026 reinforces the importance of ransomware, vulnerability exploitation, supply-chain compromise, unauthorized access and the growing role of AI. For GRC, the most useful framing is dependency risk: critical business services depend on identity providers, cloud platforms, SaaS, APIs, software components, vendors, data sources and AI providers.

Build a Critical Dependency Register

- Identity provider and authentication dependency
- Cloud platform and region
- Critical SaaS providers
- External APIs
- Critical packages/components
- Support and managed-service vendors
- External data sources
- AI models/providers
- Recovery or exit option

CYBERJA SKILL PATH

Conduct cloud adoption security risk assessments

Help organizations identify cloud risks, control gaps, business impacts and treatments before and during cloud adoption.

[Explore Cloud Adoption Risk Assessment ->](#)

[ENISA Threat Landscape resources](#)

5 | Software Supply-Chain Risk Is Increasingly an Identity Problem

Modern supply-chain attacks frequently target developer accounts, package-publishing tokens, CI/CD identities and repository credentials. The software may be the target, but identity is often the pathway.

ASSESSMENT

Map the software trust chain

Developer -> Repository -> Pipeline -> Package -> Artifact -> Cloud -> Production. Identify the identity or token authorizing every transition. Shared, long-lived and highly privileged credentials should become governance findings.

CYBERJA SKILL PATH

Take a practical Zero Trust approach

Apply explicit verification and least privilege across identities, workloads, applications and software-delivery trust relationships.

[Explore Practical Zero Trust Implementation ->](#)

6 | Ransomware Defense: Focus on Behavior, Not Brand

Threat actors can switch ransomware payloads while keeping similar post-compromise techniques. Defensive maturity therefore depends less on recognizing a ransomware family and more on detecting the chain: initial access -> credential theft -> privilege escalation -> lateral movement -> defense evasion -> exfiltration -> encryption.

WORKSHOP IDEA

Hide the ransomware name

Give students only behavioral evidence - unusual authentication, privileged use, remote tooling, credential dumping, lateral movement, backup access and outbound transfers. Ask where the organization could have broken the chain.

CYBERJA SKILL PATH

Apply a 360-degree cybersecurity approach

Connect governance, people, process, technology and business risk to understand the full attack chain.

[Explore the Holistic Cybersecurity Professional path ->](#)

7 | AI Is Changing the Economics of Cybercrime

AI does not need to invent an entirely new attack class to increase cyber risk. It can reduce attacker skill requirements, labor, reconnaissance time and language barriers while packaging multiple capabilities into commercially usable services.

RISK ASSESSMENT

Ask a better AI-risk question

Do not ask only: 'Does AI create a new attack?' Also ask: 'Does AI make an existing attack easier, cheaper, faster or more scalable?' That change can materially affect likelihood.

CYBERJA SKILL PATH

Apply InfoSec industry best practices

Use recognized cybersecurity and GRC practices to translate emerging threats into practical controls, assessments and business decisions.

[Explore Cybersecurity & GRC Best Practices ->](#)

This Week's GRC Action: Authentication Flow & Token Governance Assessment

Select your primary cloud identity platform and review four layers. The goal is to move from 'Did MFA happen?' to 'Was the authentication flow appropriate, is the resulting session trustworthy, and should this action be permitted?'

Layer	Review	Key evidence
Authentication	Permitted flows, phishing resistance, exceptions	Conditional Access / IdP settings
Token	Token types, lifetime, refresh and revocation	Token policies
Session	Monitoring, device context, session termination	Sign-in and session logs
Authority	What the session can actually do	Roles, OAuth scopes, API permissions

IMMEDIATE TEST

Check device-code authentication

Determine who genuinely needs it, which applications require it, and whether everyone else can be blocked.

CyberJA Workshop: The MFA-Protected Account That Was Still Compromised

A financial-services employee receives instructions to complete a new authentication configuration. The employee uses the legitimate Microsoft authentication process and completes MFA. No password is stolen. Twenty minutes later the SOC sees a new device, Graph reconnaissance, mailbox searches, inbox rules, SharePoint downloads and AI-assisted analysis of financial correspondence.

Student challenge

- Explain how access was obtained
- Explain why MFA did not prevent the compromise
- Identify token/session control failures
- Apply Zero Trust principles
- Identify IAM evidence to collect
- Design immediate containment
- Assess business information exposed

- Improve Conditional Access
- Map controls to NIST CSF 2.0
- Prepare an executive briefing

CAREER APPLICATION

Transition from analyst thinking to senior GRC judgement

This exercise requires evidence analysis, control design, risk translation, stakeholder communication and executive reporting.

[Explore Practical Requirements of a GRC Professional ->](#)

CyberJA Career & Practice Lab

Practical on-the-job skills I developed over the years that have strengthened my InfoSec career and helped me add value to businesses and organizations.

01	Cybersecurity Assessments Assess security maturity, gaps and priorities. Explore this CyberJA learning path
02	InfoSec & GRC Best Practices Apply industry best practices to business security and governance. Explore this CyberJA learning path
03	Zero Trust Implementation Build practical Zero Trust strategy and architecture. Explore this CyberJA learning path
04	360-Degree Cybersecurity Connect people, process, technology, governance and risk. Explore this CyberJA learning path
05	IAM Governance Implement lifecycle governance, least privilege and access assurance. Explore this CyberJA learning path

06	Cloud Risk Assessment Help organizations adopt and operate cloud securely. Explore this CyberJA learning path
07	AI Risk Management Integrate AI while managing security and business risk. Explore this CyberJA learning path
08	Senior GRC Capability Develop practical skills expected in senior GRC roles. Explore this CyberJA learning path
09	Compliance Management Implement and manage an effective compliance program. Explore this CyberJA learning path
10	IT Auditing Use auditing to deepen cybersecurity and assurance skills. Explore this CyberJA learning path

Continue Your CyberJA Journey

Use the magazine to understand the issue and the CyberJA learning paths to practice the skills needed to assess, govern and communicate the risk.

CyberJA Resource Hub

Practical learning paths and resources.

[Visit resource](#)

CyberJA YouTube

Video-based cybersecurity and GRC learning.

[Visit resource](#)

RicheaPerry.com

CyberJA and professional content.

[Visit resource](#)

CyberJA Community

GRC With Richea Perry, CyberJA Podcasts and CyberJA Discord.

[Visit resource](#)

ONE ACTION TO APPLY TODAY

Check whether device-code authentication is enabled

Identify who needs it, restrict everyone else, and verify your incident-response process can revoke sessions and tokens - not merely reset passwords.

CYBERJA CORE TEACHING MESSAGE

MFA is essential - but it is not the finish line for IAM.

Modern identity governance must continuously govern authentication flows, tokens, sessions, devices and the authority exercised after authentication.