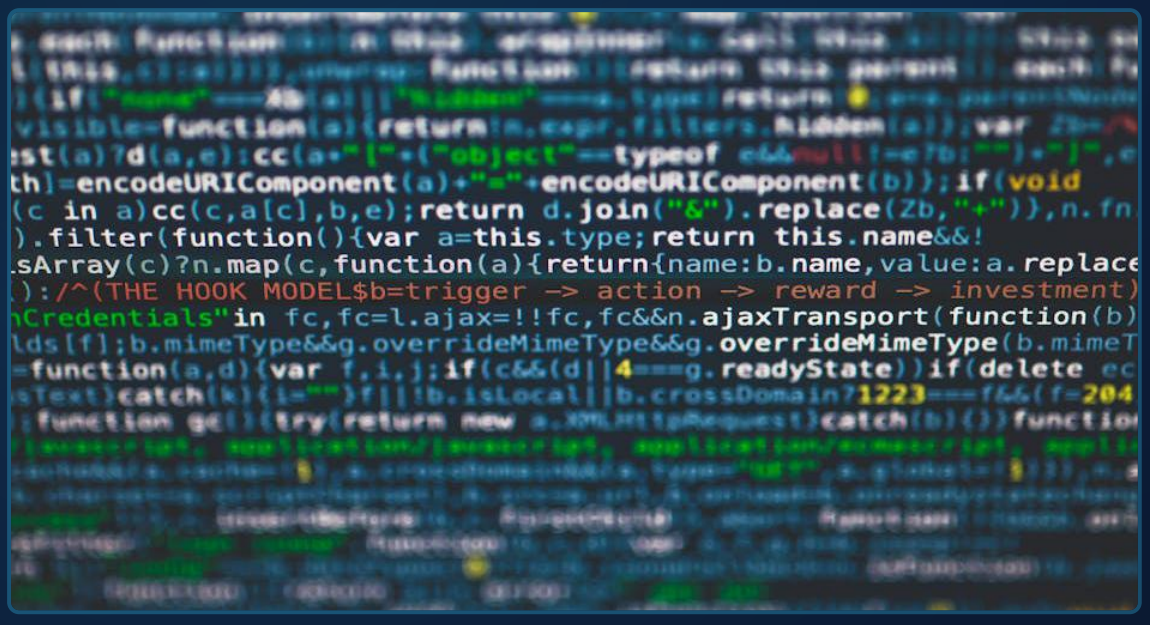
Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider



VOL. 2 · ISSUE 17

Cyber Shield

April 28, 2026

Essential cybersecurity intelligence for small and mid-sized businesses — powered by AI, delivered by Intelligent Automation, LLC.

INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

This Week in Cybersecurity

CISA Issues Emergency Directive on Critical Infrastructure Vulnerability

The Cybersecurity and Infrastructure Security Agency issued an emergency directive requiring federal agencies to patch a critical vulnerability actively exploited by threat actors targeting operational technology systems. SMBs using affected industrial control systems should apply patches immediately.

FBI

FBI Warns of Business Email Compromise Surge Targeting SMBs

Business email compromise attacks targeting small businesses rose 34% in Q1 2026. Attackers are impersonating vendors and executives to redirect payments. Multi-factor authenticati...

BLEEPING COMPUTER

Ransomware Group Expands Targeting to Healthcare and Legal Sectors

A prolific ransomware group has shifted focus to healthcare providers and law firms, sectors with lower security maturity and high data sensitivity. Average ransom demand reached 2...

INTEL

Cyber Threat Intelligence

CISA

CISA Issues Emergency Directive on Critical Infrastructure Vulnerability

The Cybersecurity and Infrastructure Security Agency issued an emergency directive requiring federal agencies to patch a critical vulnerability actively exploited by threat actors targeting operational technology systems. SMBs using affected industrial control systems should apply patches immediately.

FBI

FBI Warns of Business Email Compromise Surge Targeting SMBs

Business email compromise attacks targeting small businesses rose 34% in Q1 2026. Attackers are impersonating vendors and executives to redirect payments. Multi-factor authentication and payment verification callbacks remain the most effective defenses.

BLEEPING COMPUTER

Ransomware Group Expands Targeting to Healthcare and Legal Sectors

A prolific ransomware group has shifted focus to healthcare providers and law firms, sectors with lower security maturity and high data sensitivity. Average ransom demand reached 2.3M in verified incidents this quarter.

INTEL

Threat Intelligence — Continued

KREBS ON SECURITY

New Phishing Campaign Spoofs Microsoft 365 Login Pages at Scale

Security researchers identified a large-scale phishing campaign using adversary-in-the-middle techniques to bypass MFA on Microsoft 365 accounts. The campaign has targeted over 10,000 organizations.

DARK READING

Critical Zero-Day Found in Widely Used VPN Software

A critical zero-day vulnerability has been discovered in a widely deployed enterprise VPN solution. Threat actors are actively exploiting the flaw to establish persistent access before patches are applied.

CISA KEV

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA added three actively exploited vulnerabilities affecting enterprise software to its Known Exploited Vulnerabilities catalog, requiring federal agencies to remediate within two weeks.

CISA / NSA

Joint Advisory: PRC-Linked Threat Actors Targeting US Infrastructure

A joint advisory from CISA, NSA, and FBI warns that PRC state-sponsored actors are pre-positioning on US critical infrastructure networks for potential disruptive attacks.

WEEKLY TECH TIP

Spot Fake Login Pages Before Surrendering Your Credentials

Phishing campaigns increasingly use convincing replicas of Microsoft 365 and other common login pages to steal employee credentials. A moment of verification can prevent a costly breach that compromises your entire organization.

Step 1: Always check the URL in your browser's address bar before entering credentials.

Step 2: Bookmark legitimate login pages and access them only through your saved bookmarks.

Step 3: Enable multi-factor authentication on all business accounts to block stolen passwords.

Step 4: Report suspicious login requests to your IT team immediately, even false alarms.

ALERTS

National Cybersecurity Alerts

CISA KEV

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA added three actively exploited vulnerabilities affecting enterprise software to its Known Exploited Vulnerabilities catalog, requiring federal agencies to remediate within two weeks.

CISA / NSA

Joint Advisory: PRC-Linked Threat Actors Targeting US Infrastructure

A joint advisory from CISA, NSA, and FBI warns that PRC state-sponsored actors are pre-positioning on US critical infrastructure networks for potential disruptive attacks.

HHS / CISA

Healthcare Sector Alert: Scattered Spider Targeting Hospital Networks

CISA and HHS issued an alert warning healthcare organizations about the Scattered Spider threat group actively targeting hospital IT help desks using social engineering tactics.

REGIONAL

Regional & Sector-Specific Alerts

CISA KEV

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA added three actively exploited vulnerabilities affecting enterprise software to its Known Exploited Vulnerabilities catalog, requiring federal agencies to remediate within two weeks.

CISA / NSA

Joint Advisory: PRC-Linked Threat Actors Targeting US Infrastructure

A joint advisory from CISA, NSA, and FBI warns that PRC state-sponsored actors are pre-positioning on US critical infrastructure networks for potential disruptive attacks.

HHS / CISA

Healthcare Sector Alert: Scattered Spider Targeting Hospital Networks

CISA and HHS issued an alert warning healthcare organizations about the Scattered Spider threat group actively targeting hospital IT help desks using social engineering tactics.

APRIL AWARENESS

Data Privacy Month

Security Awareness Spotlight: Data Privacy Month April is Data Privacy Month, and it's the perfect time to take stock of what customer and business information you're holding onto. Many small businesses collect more personal data than they need and keep it longer than necessary, which increases your risk if there's ever a breach or compliance audit. Take 30 minutes today to list every place you store customer information—from email inboxes and spreadsheets to payment systems and cloud folders—then delete any data you no longer need and restrict employee access to only what each person requires for their job.

ACTION ITEM

Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

Protecting Your Business

SMB SPOTLIGHT

Why SMBs Are Now the Primary Target — And What to Do About It

Cybercriminals have learned that small businesses offer an attractive combination: valuable data, inadequate defenses, and willingness to pay ransoms. The good news is 85% of successful attacks exploit preventable weaknesses.

INSURANCE JOURNAL

The .88M Question: Why Cyber Insurance is Now Non-Negotiable for SMBs

The average cost of a data breach hit .88M in 2025. For small businesses, a single incident can be fatal. Cyber insurance has evolved from optional to essential risk management.

NIST

Password Managers: The 30-Minute Investment That Prevents 80% of Breaches

Security experts agree: deploying a password manager is the single highest-ROI security investment for small businesses. Teams that use them see dramatically fewer credential-based compromises.

INNOVATION

Cybersecurity Advancements

MICROSOFT

Microsoft Copilot for Security Now Available to All M365 Business Customers

Microsoft has made its AI-powered security copilot available to all Microsoft 365 Business customers, bringing enterprise-grade threat detection to small business plans.

GOOGLE BLOG

Google Announces Passkey Adoption Reaches 1 Billion Users

Google reports that passkey authentication has surpassed 1 billion users globally, marking a major milestone in the industry's push to eliminate password-based authentication.

NIST

NIST Releases Final Post-Quantum Cryptography Standards

NIST has published the final post-quantum cryptography standards, giving organizations a clear roadmap to protect their encrypted data against future quantum computing threats.

CTO'S DESK

From the Desk of Daniel Ramos

Daniel Ramos
Chief Technology Officer
Intelligent Automation, LLC | Fairfield, NJ
Managed Cybersecurity Service Provider

This week's headlines paint a concerning picture, but there's one thread connecting nearly every story: attackers are increasingly exploiting the human element and trusted systems we use every day.

Whether it's the Microsoft 365 phishing campaign or the surge in business email compromise, cybercriminals aren't necessarily getting more sophisticated—they're getting smarter about manipulating trust. They know that a well-crafted email from what appears to be your CEO or a familiar login page is often all it takes to bypass even the best technical defenses.

The CISA emergency directive and VPN zero-day remind us that patching matters, absolutely. But here's what I want you to remember: your people are both your greatest vulnerability and your strongest defense. The same employee who might click a malicious link today can become your first line of detection tomorrow with proper training and awareness.

I encourage you to have a five-minute conversation with your team this week about these threats. Make it real. Show them examples. Security awareness doesn't require a massive budget—it requires consistent attention and a culture where everyone feels responsible for protecting what we've built together.

CONNECT WITH DANIEL
linkedin.com/in/iamdanielramos · daniel.ramos@intelamation.com

Your Cybersecurity Partner for the Digital Age

Serving small and mid-sized businesses since 2013

336 US Highway 46, Fairfield, NJ 07004

(888) 711-4521 · intelamation.com

Read online: newsletters.intelamation.net