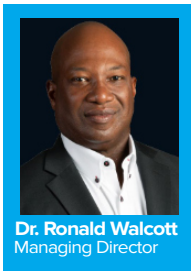
precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 49 SEPTEMBER 2025

Cybersecurity Awareness – Secure Our World



Dr. Ronald Walcott
Managing Director

As the calendar turns to October, we officially usher in Cybersecurity Awareness Month, a crucial time to dedicate our focus to the digital safety of ourselves, our families, and our organization. This year's powerful theme, "Secure Our World," reminds us that the responsibility of digital defense extends far beyond the security team—it belongs to every one of us, whether we are managing critical business data or simply browsing on a personal device. This month, we will be dedicating our newsletter to providing you with practical knowledge, essential tools, and critical, actionable insights designed to strengthen your digital habits, recognize modern threats, and collectively build a more resilient and protected environment for everyone.

EVERYDAY ESSENTIAL TOOLS THAT BUILD A RESILIENT ENVIRONMENT

Everyday essential tools for building a resilient digital environment focus on reducing the attack surface, controlling access, and providing a rapid recovery mechanism. Discussing three core tools—Password Managers, Multi-Factor Authentication (MFA), and Automated Cloud Backups—highlights this essential defense strategy.

1. Password Managers

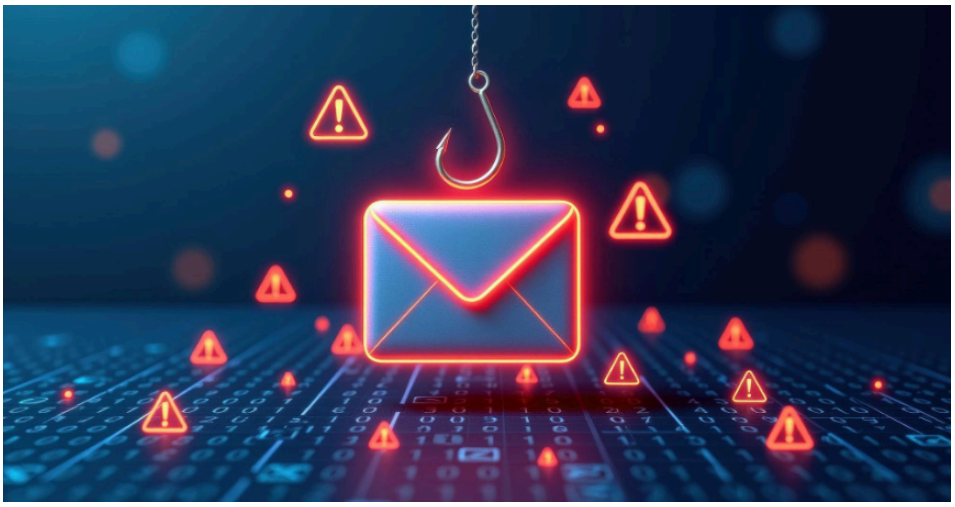
Password managers are the foundation of identity security, solving the human tendency to reuse or create weak credentials.

- **Enforce Unique, Complex Credentials:** They automatically generate and securely store unique, long, and complex passwords for every single service. This eliminates the risk of "credential stuffing," where a breach on one site compromises a user's account across dozens of others.
- **Prevent Phishing and Man-in-the-Middle Attacks:** High-quality password managers (like browser extensions) can only auto-fill credentials when the user is on the correct, registered URL. If a user lands on a look-alike phishing site, the manager will not offer to fill the credentials, providing a subtle but powerful defense against deception.
- **Centralized Security Auditing:** Most modern managers include a security dashboard that actively scans the user's stored passwords, alerting them to any compromised, reused, or weak passwords, and prompting them to update them immediately.

2. Multi-Factor Authentication (MFA)

MFA, particularly hardware or app-based MFA, is the single most effective control against unauthorized access, even if a password is stolen.

CONTINUED ON PAGE 2



IN THIS ISSUE:

- **Mitigate Stolen Passwords:** Even if an attacker successfully acquires a username and password (through phishing, malware, or a breach), they cannot gain access without the second factor (the code from the authenticator app or the physical security key). This renders credential theft virtually useless.
- **Resilience Against Session Hijacking:** The most secure forms of MFA, specifically hardware security keys (like YubiKey) using the FIDO protocol, provide resilience against sophisticated attacks like "session hijacking" or real-time phishing. These physical keys cryptographically verify the origin of the login request, ensuring the user is interacting with the legitimate service.
- **Simple and Widespread Deployment:** Major services like Google, Microsoft, and countless others natively support MFA. Integrating a single authenticator app (like Google Authenticator or Microsoft Authenticator) or a security key across all essential accounts is easy and adds significant protective layering.

3. Automated Cloud Backups

Automated backups are the ultimate tool for organizational resilience, guaranteeing business continuity and data integrity following a destructive event like ransomware or hardware failure.

- **Protection Against Ransomware:** If a system is locked or encrypted by ransomware, a complete, isolated, and tested cloud backup allows the organization or user to wipe the infected system and restore their data to a pre-infection state, bypassing the need to pay the ransom.
- **Ensure Data Immutability and Off-Site Storage:** Modern cloud backup services offer "immutable" storage, meaning backup data cannot be altered or deleted by a malicious actor (or a ransomware process) once it is stored. Furthermore, storing the backup off-site in the cloud protects against localized disasters like fire or flood.
- **Minimize Downtime (Business Continuity):** Automated, scheduled backups ensure that the Recovery Point Objective (RPO)—how much data can be lost—is minimized. When a failure occurs, the data is readily available for quick restoration, significantly reducing costly business downtime.

CYBERSECURITY AWARENESS

Let's look at how to leverage Cybersecurity Awareness Training to recognize modern threats requires focusing on the shift from generic rules to practical, context-aware threat identification. Here are three key points:

1. Training on Contextual Phishing and Vishing Recognition

Modern threats have evolved beyond simple spelling errors in emails. Training must focus on contextual anomalies in sophisticated phishing and vishing (voice phishing) attempts.

- **Focus Point:** Employees should be trained to scrutinize the context of a request, not just the sender's email address. This includes teaching them to spot social engineering cues like an urgent request for a wire transfer from a C-level executive, a sudden change in vendor bank details, or an HR request for personal information that falls outside standard procedure.
- **Method:** Utilizing simulated phishing campaigns is crucial, especially those that mimic real, recent threats seen in the industry or specific to the company (e.g., invoice fraud, "CEO fraud").1 The training should also cover vishing techniques, teaching users to verify unexpected calls asking for sensitive information by hanging up and calling back on a known, official line.

2. Recognizing Supply Chain and Third-Party Risk

As organizations rely heavily on external software and vendors, threats now commonly enter through the supply chain, requiring specialized training to recognize and mitigate.2

- **Focus Point:** Training should educate employees on the concept of supply chain compromise, where legitimate software updates or dependencies are poisoned with malicious code.3 Employees need to understand that trust in a well-known vendor is not absolute, and they must be vigilant regarding unexpected changes.
- **Method:** This involves teaching technical staff (developers, operations) about secure coding practices and dependency checking tools (Software Composition Analysis), while teaching procurement and legal teams how to properly vet vendor security posture and identify red flags in their access and integration requests. For all employees, it means reporting any unusual behavior from trusted applications immediately.

3. Understanding Initial Access Broker (IAB) Techniques

Modern attackers often don't execute the final attack (like ransomware) themselves; they specialize in gaining and selling initial network access, making awareness of these techniques vital.4

- **Focus Point:** Employees need to be aware of the subtle techniques used by Initial Access Brokers (IABs) to gain a foothold, which often involve using common, legitimate tools (living off the land) rather than introducing new malware. This includes recognizing and reporting unauthorized RDP connections, excessive use of PowerShell or scripting tools, and changes to firewall rules.
- **Method:** Training should emphasize endpoint vigilance and least-privilege principles. Employees should be educated that leaving a remote desktop (RDP) connection exposed or using a default password on a network device is a critical gateway for an IAB.5 The goal is to make every employee a sensor for unusual network activity related to remote access and administrative tools.

Frequently Asked Questions:

HOW CAN WE STRENGTHEN OUR DAILY HABITS TO IMPROVE OUR CYBER SECURITY POSTURE?

Improving your cybersecurity posture starts with making stronger habits your default actions, moving beyond simply relying on tools. The most impactful changes involve ditching password reuse entirely by using a password manager to create and store unique, complex credentials for every account. You must also enable Multi-Factor Authentication (MFA) on all sensitive platforms—especially email, banking, and social media—as this single step blocks the vast majority of account takeover attempts. Finally, adopt a habit of skepticism toward unexpected communications, whether it's an urgent email from an unknown sender or a surprising link from a colleague, and practice the "Stop, Look, and Think" approach before clicking, downloading, or entering any credentials.

WITH THE RISE OF AI TECHNOLOGIES, HOW DO HUMANS COMBAT THE THREATS AI POSES?

Combating threats posed by the rise of AI requires a multi-faceted approach centered on human vigilance, regulatory frameworks, and AI-assisted defense. Humans must prioritize education to recognize highly sophisticated, personalized threats, such as deepfake media and AI-generated phishing, and develop new auditing skills to scrutinize the output of generative models for bias or malicious intent. Crucially, we must push for the development and adoption of AI-driven defense mechanisms—using AI to rapidly detect and counter other adversarial AI systems—while simultaneously enacting clear ethical and legal guidelines that enforce transparency, accountability, and traceable watermarking on synthetic content to ensure we can distinguish between real and AI-generated information.

WHAT CAN WE DO IN THE CARIBBEAN TO ENSURE CYBERSECURITY IS TAKEN SERIOUSLY?

To ensure cybersecurity is taken seriously across the Caribbean, the region must shift its focus from reactive cleanup to proactive, collaborative investment. This involves harmonizing national cybersecurity policies and establishing regional centers for threat intelligence sharing, allowing islands to collectively combat threats that cross borders. Governments and the private sector must prioritize mandatory, localized training and certification programs to address the critical shortage of skilled professionals, effectively treating cybersecurity not just as an IT issue but as an essential national and economic security priority. Finally, there needs to be a unified push for stronger regulatory compliance that includes significant penalties for data breaches, compelling organizations to invest in foundational security measures like Multi-Factor Authentication (MFA) and routine patching.

WHY CLIENTS CHOOSE US

We offer companies a complete, top to bottom approach to assess posture, identify gaps, implement securities and mitigate risk.

precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

UPCOMING EVENTS

GRRCON CYBER SECURITY SUMMIT AND HACKER CONFERENCE
MI, USA – October 2nd, 2025

OWASP GLOBAL APPSEC US
Washington, D.C., USA – November 3rd – 5th, 2025

SECURE CAROLINAS CONFERENCE 2025
Raleigh, NC, USA
December 2nd – 3rd, 2025

Headline News

AI Agents Drive New Security Demands

Artificial intelligence agents have rapidly become a force inside enterprises, creating a surge of new, non-human identities. While adoption has grown quickly, oversight has not kept pace. More than 80% of organizations now use agents, but only 40% actually manage them, said Steve Bradford, senior vice president and general manager for EMEA at SailPoint. That lack of control is leading to unauthorized access and exposing sensitive data.

The challenge, Bradford said, lies not only in securing agents but also achieving faster returns on identity investments. Many enterprises remain stuck in early maturity phases. He called for broader visibility across the long tail of applications to improve control and ROI.

"More than 80% of companies that are using agents say they have had unauthorized access to data, and yet they're still at a stage where they don't quite know how to take advantage of the benefits of those agents and secure them at the same time," he said.

In this video interview with Information Security Media Group at Gartner Security & Risk Management Summit London, Bradford also discussed:

- How agentic AI shifts identity security from humans to machines;
- The importance of managing SaaS applications at scale;
- SailPoint's efforts to close the skills gap through online resources and in-person training.

Bradford leads EMEA go-to-market teams at Sailpoint. He has more than 30 years of IT experience, including nearly 25 years in enterprise software and SaaS. He has held executive roles at IBM, SAP, Salesforce, ServiceNow and Automation Anywhere.

Soure: www.databreachtoday.com

868-610-7237

info@precision-cyber.com

www.precision-cyber.com

1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad