Cybersecurity Awareness Month 2026: What Industry Experts Want You to Know

vmblog.com/bylines/cybersecurity-awareness-month-2026-what-industry-experts-want-you-to-know

David Marshall

October is Cybersecurity Awareness Month, and if the last twelve months have proven anything, it's that the threat landscape isn't slowing down to observe it. From AI-powered phishing campaigns and deepfake-driven social engineering to the steady drumbeat of ransomware attacks hitting hospitals, schools, and municipalities, security teams have had precious little downtime in 2026. This annual observance, now in its third decade, remains one of the industry's best excuses to pause, take stock, and ask: are we actually getting safer, or just busier?

To mark the occasion, VMblog reached out to security leaders, CISOs, researchers, and vendors across the industry to get their take on where things stand. What follows is a round up of that commentary — perspectives on the trends shaping defense strategies, the mistakes still tripping up organizations of every size, and the practical steps security teams can take to close the gap between awareness and actual resilience.

As always with our round ups, the goal isn't a single unified message — it's a snapshot of where the industry's collective head is at right now, in the experts' own words.

++

Kevin Walker, Founder and Senior Cyber Security Consultant, Black Swan Cyber Security Solutions

Heading into Cybersecurity Awareness Month 2026, I wonder whether awareness itself is really the problem. Most people know cybercrime exists. They've heard about phishing, ransomware and dodgy links. Where organisations still struggle is turning all that awareness into everyday security. MFA, patching, tested backups, sensible access controls and good email security aren't particularly exciting, but they mean one convincing email or one momentary lapse doesn't have to become a major incident.

I'd also like to see the cyber industry retire the phrase "people are the weakest link". Attackers exploit perfectly normal human behaviour: trust, curiosity, urgency, helpfulness and the pressure of a busy working day. AI is making convincing emails, messages and impersonation much easier to produce. We can't keep responding by telling people to "be more careful". Give them sensible technical safeguards, make it easy to question something that doesn't feel right and, importantly, create a culture where someone can put their hand up quickly when they think they've made a mistake.

That's particularly important for the schools and smaller organisations I work with. They don't have unlimited budgets or teams of cyber specialists. Good cyber security for them means getting the basics right, layering sensible controls and knowing what they're going to do when something gets through. Perhaps that's the question Cybersecurity Awareness Month should leave us with this year: instead of asking how we stop people making mistakes, how do we stop one mistake becoming a disaster?

++

Stefan Ristić, Founder, TLDWP & WordPress Security and Infrastructure Specialist, TLDWP

Cybersecurity Awareness Month is often framed around awareness, but heading into 2026, I think the bigger gap is turning awareness into routine operational hygiene. TLDWP's current security baseline covers more than 7.4 million detected WordPress sites. Of the sites checked for security headers, 82.5% receive an F in our six-header grading model, while more than 132,000 expose at least one file or directory we track. We also currently observe over 113,000 publicly accessible phpinfo/info.php pages and more than 6,700 exposed debug.log files. None of these signals alone means a website is compromised, but at this scale they show how much avoidable exposure remains on the public web.

The lesson is that cybersecurity awareness cannot stop at telling people to use MFA and install updates. Organizations need ownership of the less glamorous controls: knowing what assets are online, keeping them patched, removing debug artifacts, reducing unnecessary public exposure, reviewing access, and verifying those controls continuously. In incident-response work, I repeatedly see how small weaknesses become much more serious when they accumulate or when attacker persistence is only partially removed. Awareness matters, but real improvement comes when those practices become operational habits rather than an annual reminder.