Concierge Digital Solutions

CDS Tech Tips

Monthly Security & Technology Insights

As we head into September 2026,

we're seeing a significant uptick in AI-powered phishing attacks and critical vulnerabilities across enterprise platforms. Here's what you need to know to protect your business.

— Ron Willitzer

⚠ SECURITY ALERT

AI-Enhanced Phishing Campaigns Hit 5-Year High

September 2026 marks a turning point in phishing sophistication. Advanced AI tools are generating hyper-personalized emails that bypass traditional filters. Unlike generic phishing, these attacks are **deeply researched**—referencing real projects, client names, and internal processes. Threat actors are using leaked corporate data combined with generative AI to craft emails that pass human scrutiny.

Key indicators we're seeing:

- Personalized greetings using employee names and titles
- References to recent company news or projects
- Requests for urgent verification via fake portals
- Invoices and payment requests with company branding
- Impersonation of known vendors and partners

Your defense: We monitor and filter these threats 24/7 for all CDS clients. However, user education is critical. Never click links or download attachments from unexpected emails—even if they appear to come from trusted contacts. When in doubt, verify by calling the sender directly using a known phone number.

🔧 CRITICAL UPDATES

Windows & Apple Release Emergency Patches

Both Microsoft and Apple released critical security updates this month addressing active vulnerabilities.

Windows (September Patch Tuesday): Microsoft released 487 security fixes including 4 zero-day vulnerabilities being exploited in the wild. The most critical affects Windows 11 and Windows 10, potentially allowing remote code execution through Windows Server Message Block (SMB) protocols.

Mac & iPad (September 17, 2026): Apple released macOS Tahoe 26.9 and iOS 26.8, addressing 31 security vulnerabilities. Updates are available for macOS, iOS, iPadOS, and watchOS. Earlier device versions also received patches: macOS 13.x (Big Sur) and iOS 18.7 received critical backports.

What to do: Enable automatic updates on all devices. If you manage Windows systems, we recommend deploying these patches within 48 hours given the active exploits. CDS clients receive these patches

automatically through our managed services.

SAFE INTERNET PRACTICES

3 Things to Do This Month

1. **Enable Two-Factor Authentication (2FA)** If you haven't already, enable 2FA on your critical accounts: email, banking, and work systems. This is the single strongest defense against credential theft. We can help configure this securely.

2. **Review Backup Status** Verify your backups are running and recoverable. Test restoring a file to ensure backups are working properly. Ransomware is increasingly targeting backups—we manage this for you.

3. **Update All Browsers & Extensions** Check your browsers (Chrome, Safari, Firefox, Edge) for updates. Remove unused extensions—they're often overlooked attack vectors. We can audit your browser security posture.

Questions about these threats? Need help deploying patches or implementing security best practices?

Schedule Security Consultation

832-378-8393

September's Landscape: The convergence of AI-powered phishing and zero-day exploits creates a perfect storm. The best defense combines automated threat detection (which we provide), timely patch deployment, and human awareness. CDS clients benefit from 24/7 monitoring, automatic patching, and immediate incident response if a breach occurs.

Concierge Digital Solutions

Keeping your technology running smoothly since 2017

832-378-8393 | ron@cdsolutions.net

www.cdsolutions.net