Concierge Digital Solutions

CDS Tech Tips

Monthly Security & Technology Insights

Hello from CDS,

June brings summer plans—and sophisticated cyber threats. This month's newsletter covers AI-powered phishing attacks, critical system vulnerabilities, and essential password management best practices to keep your digital summer secure.

CRITICAL ALERT

AI-Powered Social Engineering: The New Phishing Frontier

Cybercriminals continue to leverage artificial intelligence to craft increasingly sophisticated social engineering attacks. June marks a significant rise in targeted AI-generated phishing campaigns that mimic legitimate business communications with alarming precision.

What makes these attacks dangerous:

- **Personalized content** — AI analyzes social media and public data to create messages tailored to specific individuals and companies
- **Perfect messaging** — grammatically flawless emails that blend in with legitimate correspondence
- **Urgent language** — designed to bypass logical thinking and trigger immediate emotional responses
- **Convincing sender spoofing** — emails that appear to come from executives, vendors, or trusted partners
- **Multi-channel attacks** — phishing via email, SMS, social media, and messaging apps simultaneously

Your defense: Verify any financial or sensitive requests directly with the sender using a known contact method—not the contact info in the suspicious message. Enable multi-factor authentication (MFA) on all critical business accounts. Train employees to recognize urgency tactics and unusual payment instructions.

SECURITY UPDATES

Critical Updates: Windows Kernel & Apple Safari Patches

Both Microsoft and Apple have released emergency updates addressing actively exploited vulnerabilities. Prioritize these patches immediately—they're critical to your system security.

Windows users: Install KB5032195 (June security update) addressing a critical Windows kernel vulnerability (CVE-2024-21418) that allows privilege escalation. This affects all recent Windows versions and is actively being exploited. Go to Settings > Update & Security > Windows Update and install all available updates immediately.

Apple users: Update to macOS 13.5, iOS 17.5, and Safari 17.5 to patch multiple vulnerabilities including zero-days in Safari's WebKit engine. These patches fix over 40 security issues. Go to System Settings >

General > Software Update (Mac) or Settings > General > Software Update (iPhone/iPad).

Browser users (all platforms): If using Safari, Chrome, Firefox, or Edge, update immediately. Browser vulnerabilities are prime targets for attackers. You should see update prompts, or check the settings menu for your specific browser.

QUICK TIPS

3 Things to Do This Month

1. **Upgrade your password manager.** Switch to enterprise-grade solutions like 1Password or integrate Apple Keychain with iCloud Keychain for stronger encryption. Avoid storing passwords in browsers or email. Complex, unique passwords for every account are non-negotiable in 2026.

2. **Audit your browser extensions.** Malicious extensions are a primary attack vector. Remove any unused extensions, disable those you don't trust, and only install from official app stores (Chrome Web Store, Firefox Add-ons, Safari App Store). Verify the developer's legitimacy before installing.

3. **Enable multi-factor authentication (MFA).** Require MFA on email, banking, business clouds (OneDrive, Google Drive, iCloud), and social media accounts. This single step blocks 99.9% of account takeover attempts. Authenticator apps (Microsoft Authenticator, Google Authenticator) are more secure than SMS.

Not sure if your systems are fully patched or your security posture is strong enough?

📞 832-378-8393

Get a Security Audit

Concierge Digital Solutions

Keeping your technology running smoothly since 2017

832-378-8393 | ron@cdsolutions.net

www.cdsolutions.net