



Concierge Digital Solutions

CDS Tech Tips

Monthly Security & Technology Insights

Hi there from the CDS team,

October brings a new wave of AI-driven phishing tactics spreading beyond email into everyday work chat, plus critical patches from Apple and Microsoft worth knowing about. Here's what's changed and what we're doing to keep you covered.

— Ron Willitzer

⚠ SECURITY ALERT

Phishing Has Moved Beyond Email — Now It's Teams Messages and Phone Calls

The obvious phishing email — bad grammar, broken links, strange formatting — is nearly extinct. Attackers are using AI to write messages that sound natural and reference real details about your business, and they're no longer sticking to the inbox. Microsoft's latest threat research flagged a rise in attackers impersonating coworkers and IT staff through Teams messages and phone calls, where people naturally let their guard down.

Red flags to watch for:

- An "urgent" request to approve a payment, change banking details, or buy gift cards
- A message from a coworker or vendor that feels slightly off, even if the writing looks polished
- A call or chat message claiming to be "IT support" asking for a password or remote access
- Pressure to bypass normal approval steps or keep a request confidential
- A sudden request to update a password or payment method via a link

What to do: Don't click, reply, or approve anything — call us immediately. We monitor and filter these threats 24/7 for all CDS clients, and we'd always rather confirm something is safe than have you guess wrong.

Apple & Microsoft Released Critical Security Patches

Both Apple and Microsoft shipped significant security updates recently, and both are worth having installed.

Apple (macOS & iOS): Updates for macOS Tahoe, Sequoia, and Sonoma, plus iPhone and iPad, address a serious Screen Sharing vulnerability that could let an attacker take control of a Mac without a valid password. Researchers found tens of thousands of exposed Macs reachable over the internet before the fix went out.

Microsoft (Windows): The latest monthly security update addressed over 900 vulnerabilities, including more than 100 rated critical and two that attackers were already actively exploiting before the patch was released.

What to do: If your device is managed by us, you're already covered — we patch all managed devices automatically. If you're unsure about a personal or unmanaged device, give us a call and we'll check it for you.

SAFE INTERNET PRACTICES

3 Things Worth Checking This Month

1

Confirm Two-Factor Authentication Is On Email, banking, and work accounts should all have it enabled. It remains the single most effective way to stop a stolen password from turning into a real breach. We can audit your accounts and set it up securely.

2

Verify Your Backups Actually Work A backup that's never been tested can give a false sense of security. We verify recoverability for all our managed clients — if you'd like us to check yours, just ask.

3

Review Who Still Has Access Former employees, old vendor logins, and unused admin accounts are an easy way in for attackers. We recommend a periodic access review — reach out if it's been a while.

Have a question or need help with any of this? We're just a call or email away.

[Schedule Security Consultation](#)

October's Landscape: AI is closing the gap between "obviously fake" and "looks completely legitimate" for phishing attempts — and attackers are spreading that playbook across chat and phone channels, not just email. The best defense combines layered monitoring (which we provide), fast patch deployment, and a habit of verifying unusual requests before acting on them. CDS clients benefit from 24/7 monitoring, automatic patching, and immediate incident response if something slips through.

Concierge Digital Solutions

Keeping your technology running smoothly since 2017

📞 832-378-8393 | ron@cdsolutions.net

www.cdsolutions.net

You're receiving this because you're a valued CDS client.
To unsubscribe, reply with "unsubscribe" in the subject line.