Virtual Dynamics
MANAGED IT SERVICES

THREAT BRIEF · WEEK OF NOV 16, 2026

This week in cyber, minus the jargon.

Six things that happened Nov 9–16, 2026, and the quick fix for each. Tape it by the front desk. ☕

PATCH IT
Outlook had a live zero-day.

What happened: On Nov 10, Microsoft fixed an Outlook flaw already being used in attacks. Opening a booby-trapped message file could leak your sign-in details.

Do this: Update Microsoft 365 / Office apps. This fix comes through Office updates, so check Outlook, not just Windows.

PATCH IT
Chrome got one too.

What happened: On Nov 9, Google fixed a Chrome flaw it says is being exploited in the wild.

Do this: Menu › Help › About Google Chrome, then Relaunch. You want version 157.0.8103.50 or newer.

PLAN FOR IT
Microsoft 365 had a very bad day.

What happened: On Nov 12, a nearly 24-hour outage hit Outlook, Exchange Online and Teams worldwide. Microsoft traced it to a latent bug from July, triggered when load rose and some capacity was already offline.

Do this: Keep an offline phone list for staff and key clients, and agree now how you'll reach patients or families if email is down.

SPOT IT
That "booking code" was a sign-in.

What happened: Huntress caught a fake Teams meeting scheduler that got an employee to type a real Microsoft device sign-in code, handing over their session.

Do this: Only type a code into a Microsoft page if **you** started that sign-in yourself.

SPOT IT
"Press Win+R and paste" = scam.

What happened: Fake Zillow review pages told visitors to press Windows+R, paste and hit Enter. That installed hidden remote-control software.

Do this: No real website asks you to paste a command to "verify." Close the tab and tell IT.

CHECK IT
Police seized a pile of stolen logins.

What happened: Police in nine countries, with Europol, took down malware servers and recovered over 6 million stolen logins. Some victims may get breach alerts from Have I Been Pwned.

Do this: Got a breach alert? Change that password everywhere you used it and turn on MFA.

Your firewall's homework. Advisories this week confirmed attacks on internet-facing security gear, including Check Point gateways and Barracuda email gateways. Ask your IT provider two questions: **Is our firewall and VPN firmware current? Does remote access require MFA?**

DATES TO CIRCLE

Jan 13, 2027
Windows Server 2016 support ends. Still running one? Plan the move now.

Feb 1, 2027
Microsoft retires its own text & voice sign-in codes for most users. People who still rely only on those codes will be asked to set up a passkey.

Nov & Dec 2026
"No-reboot" hotpatched Server 2022 machines still need a restart for these two updates.

Holiday shipping
USPS won't text you links, even if you signed up for tracking. Forward fake delivery texts to 7726.

Sources: Microsoft Security Response Center & BleepingComputer (Outlook CVE-2026-124194, Nov 10); Google Chrome Releases (Nov 9); CISA Known Exploited Vulnerabilities alerts (Nov 10 & 13); BleepingComputer (Microsoft 365 outage, Nov 16; Check Point, Nov 13); Huntress (Nov 12) & Help Net Security (Nov 13); Help Net Security (fake Zillow pages, Nov 13; Operation Endgame, Nov 12); Europol; Microsoft Learn (Windows Server 2016 lifecycle; SMS & voice retirement); Microsoft message MC1527979; FCC (package delivery scams). Facts current as of Nov 16, 2026.

Questions? Just ask us.
Plain-English answers from your Chicagoland IT team since 2010.

(888) 531-1109
vdcmsp.com