HERMES CLOUD
MANAGED IT SERVICES

VOLUME 002 • MAY 2026
AMSTERDAM, THE NETHERLANDS

TECH TALK

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE

THE "SESSION COOKIE" HIJACK: WHY MFA CAN'T ALWAYS SAVE YOU

MFA Isn't the Finish Line: The Hidden Risk of Session Cookie Hijacking

MFA is an important security layer, but it's not enough on its own. After you log in, websites keep you authenticated using session tokens (cookies), similar to a wristband that proves you've already been verified.

If attackers steal this "wristband," they can access your account without needing to pass MFA. This is called session cookie hijacking, where attackers bypass login protections by reusing an already authenticated session instead of breaking MFA itself.

The key takeaway: MFA is effective, but it's not the final line of defense. Security must also protect what happens after login, since modern attacks often work around MFA rather than directly defeating it.

HOW SESSION COOKIE HIJACKING ACTUALLY HAPPENS

01 AiTM PHISHING
Adversary-in-the-middle (AiTM) phishing tricks users into logging into a fake site that relays their login to the real service. This lets attackers steal access in real time and bypass MFA.

02 BROWSER-IN-THE-MIDDLE SESSION STEALING
It's similar in concept but more direct: instead of just stealing a password, the attacker actively takes control of the browsing session.

03 COOKIE THEFT FROM THE ENDPOINT
Session hijacking can start with a proxy or stolen session data from a device, allowing attackers to impersonate a real user.

MFA IS A BASELINE, NOT A FINISH LINE
MFA is still essential for blocking most credential theft, but it doesn't stop attacks that target active sessions. Effective security needs layered protections beyond login, especially for session security.

REMCO HERMES
OWNER

We're passionate about making technology work for you. Let's have a quick, friendly chat to see how we can enhance your IT and keep your data secure. Contact us today to schedule a consultation.

HERMES CLOUD
MANAGED IT SERVICES

VOLUME 001 • MAY 2026
AMSTERDAM, THE NETHERLANDS

THE "BACKUP EXIT" STRATEGY: CAN YOU MOVE YOUR DATA WITHOUT THE VENDOR'S HELP?

A backup exit strategy helps businesses securely move their data away from SaaS vendors without relying on costly or rushed support. Without a proper exit plan, companies risk vendor lock-in, higher costs, and limited flexibility when switching platforms. Since data migrations involve high-level access and sensitive information, businesses should strengthen security with phishing-resistant sign-ins, stricter session controls, secure devices, and active monitoring during the move.

RED FLAGS FOR FAKE RECRUITMENT SCAMS

UNCLEAR JOB DETAILS
Vague job description, unclear role details, or "we'll share specifics later."

URGENT HIRING PRESSURE
Pressure to move fast: "limited slots," "complete today," "fast-track hiring."

MOVING CONVERSATIONS OFF-PLATFORM
Push to move off LinkedIn quickly onto WhatsApp/Telegram/personal email.

REQUESTS FOR MONEY OR PAYMENTS
Requests for money, fees, gift cards, crypto, or "equipment purchases."

VERIFICATION CODE REQUESTS
Requests for verification codes.

EARLY REQUESTS FOR SENSITIVE INFORMATION
Requests for sensitive personal info early, like ID scans or bank details.

REQUESTS FOR CONFIDENTIAL COMPANY DATA
Any request for non-public company information (org charts, client lists, internal tools).

THE "LEGACY DEBT" AUDIT

Legacy debt builds up from small overlooked issues like unsupported devices, outdated software, and weak server practices, so the key is to prioritize securing internet-facing systems, replacing what's no longer supported, and isolating what can't yet be upgraded.

> *"We help turn legacy risk into control by uncovering hidden weaknesses early, so small gaps don't quietly grow into system-breaking failures later."*

"CLEAN DESK" 2.0: HOME OFFICE SECURITY DEFAULTS THAT PREVENT REAL INCIDENTS

- Auto-lock devices and manually lock when stepping away
- Never share work devices
- Secure and store laptops properly
- Keep routers updated or replace end-of-support gear
- Use MFA and strong sign-ins everywhere
- Control browser use, extensions, and updates
- Patch devices promptly and restart when needed
- Enable endpoint protection
- Treat AI automation as a controlled tool with approvals for sensitive actions
- Report suspicious activity or messages immediately

5-MINUTE SECURITY CHECK FOR BROWSER ADD-ONS

01 VET THE DEVELOPER LIKE A REAL VENDOR
If you can't clearly tell who built it and how to contact them, don'

02 READ THE DESCRIPTION LIKE A CONTRACT
If it's vague about what it does or what data it touches, treat that as a red flag.

03 PERMISSION SANITY CHECK
Broad "read and change data on all websites" access is rarely justified for a simple productivity tool.

04 WATCH FOR PERMISSION CREEP
If an extension suddenly asks for new permissions, pause.

05 DECIDE: APPROVE, AVOID, OR ESCALATE
Approve clear, least privilege tools. Avoid vague and over-permissioned ones. Escalate anything touching sensitive systems.

> *"Helpful tools should earn your trust, not quietly overreach for access."*

TECHNOLOGY TRIVIA QUESTION

Win a $50 Amazon Gift Voucher by being the first person to email us the correct answer!

What palindromic technology uses radio waves to determine location information on objects?

LAST MONTH'S ANSWER: **Trojan**

Email info@hermescloud.nl to win!

amazon

$50 GIFT CARD