

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



INSIDE THIS ISSUE

After the Login: What Happens When MFA Gets Bypassed	P1
Gadget of the Month	P1
The Hidden Cost of SaaS Backup	P2
4-Step Legacy IT Debt Audit	P2
5-Minute Browser Extension Security Check	P2
Red Flags for Fake LinkedIn Recruitment Scams	P2
Home Office Security Defaults	P2
Technology Trivia	P2

AFTER THE LOGIN: WHAT HAPPENS WHEN MFA GETS BYPASSED

MFA Protects the Login, But What Protects the Session?

Multi-Factor Authentication (MFA) remains one of the best defenses against unauthorized account access, but today's cybercriminals are finding ways around it. Rather than stealing passwords, attackers now focus on authenticated sessions, allowing them to access accounts even after MFA has been successfully completed. Protecting the login is only the first step—protecting what happens afterward is just as important.

HOW SESSION HIJACKING WORKS, AND HOW TO DEFEND AGAINST IT

01 HOW ATTACKERS GET INSIDE
Attackers use Adversary-in-the-Middle (AiTM) phishing to intercept login sessions. After a user completes MFA, they steal the active session token, allowing them to access the account without needing the password or another authentication code.

01 WHAT HAPPENS AFTER THE LOGIN?
With a stolen session, attackers can access business emails, monitor conversations, create hidden forwarding rules, and move through connected systems to steal sensitive data or launch further attacks.

01 REDUCING THE RISK
Protect your business by monitoring unusual login activity, limiting session durations, reviewing email forwarding rules, and training employees to recognize fake login pages. These simple steps help stop attackers before they can cause serious damage.

SESSION SECURITY MATTERS JUST AS MUCH

Stopping attackers doesn't end at the login screen. Protecting active sessions with continuous monitoring, user awareness, and layered security helps prevent unauthorized access after MFA has been completed.



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.

THE HIDDEN COST OF SAAS BACKUP PLAN YOUR EXIT BEFORE YOU NEED IT

Switching SaaS providers often involves hidden costs beyond monthly subscriptions. Data export fees, migration work, employee retraining, and business downtime can make changing platforms far more expensive than expected.

4-STEP LEGACY IT DEBT AUDIT

Audit your technology before technical debt becomes a business problem.

- Inventory all hardware, software, cloud services, and licenses.
- Assess operational and cybersecurity risks.
- Calculate the real cost of keeping outdated systems.
- Create a phased modernization roadmap.

THREE COSTS BUSINESSES OFTEN MISS

DATA EXPORT COSTS

Large datasets often incur significant egress charges.

MIGRATION & RETRAINING

Moving data and training employees on new platforms increases project costs.

LEADERSHIP TIME

Migration projects consume valuable management and operational resources.

RED FLAGS FOR FAKE LINKEDIN RECRUITMENT SCAMS

Watch for:

- Generic recruiter profiles
- Unrealistic salaries
- Pressure to respond immediately
- Early requests for personal information
- Moving conversations to WhatsApp or Telegram
- Requests to download unknown software
- Company information that cannot be independently verified

HOME OFFICE SECURITY DEFAULTS

Every remote worker should:

- Lock their screen when stepping away
- Enable automatic screen lock
- Remove visible passwords
- Keep desks clear of sensitive documents
- Position monitors away from public view
- Use privacy filters when needed
- Separate work and personal devices
- Maintain a dedicated workspace

5-MINUTE BROWSER EXTENSION SECURITY CHECK Before installing any browser extension:

VERIFY THE PUBLISHER

- 01** Confirm that the extension comes from a trusted developer or reputable company. Be cautious of unknown publishers or extensions that imitate well-known brands.

REVIEW REQUESTED PERMISSIONS

- 02** Check whether the extension is requesting access that matches its purpose. Excessive permissions could allow it to access sensitive information unnecessarily.

READ RECENT REVIEWS

- 03** Review recent user feedback to identify potential issues or security concerns. Pay attention to complaints about suspicious behavior or sudden changes in functionality.

CHECK UPDATE HISTORY

- 04** Make sure the extension is actively maintained and regularly updated. Frequent updates can indicate that the developer is addressing bugs and security vulnerabilities.

SEARCH FOR SECURITY CONCERNS

- 05** Look online for reports of vulnerabilities, data misuse, or security incidents involving the extension. A quick search can reveal risks that are not visible in the app store listing.

REVIEW THE PRIVACY POLICY

- 06** Read the privacy policy to understand how your data is collected, used, and shared. Avoid extensions that have unclear policies or request more information than necessary.

TECHNOLOGY TRIVIA QUESTION

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

What was the name of Microsoft's iPod competitor released in 2006?

LAST MONTH'S ANSWER:
Pac-Man

Email info@hermescloud.nl to win!



\$50 GIFT CARD