HERMES CLOUD
MANAGED IT SERVICES

VOLUME 003 • JUNE 2026
AMSTERDAM, THE NETHERLANDS

TECH TALK

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

INSIDE THIS ISSUE

WHY HUMAN HABITS ARE YOUR BIGGEST SECURITY RISK

THE BIGGEST CYBER RISK ISN'T A HACKER — IT'S HUMAN BEHAVIOR

Most cyberattacks don't begin with sophisticated malware or advanced intrusion techniques. They begin with everyday actions: clicking a personal email, reusing passwords, or uploading files through an unapproved cloud service.

Modern workplaces blend personal and professional digital activity across multiple devices, browsers, and platforms. That overlap creates opportunities for attackers to exploit human habits rather than technical weaknesses.

THE HUMAN ELEMENT IN CYBERATTACKS

01 PHISHING THRIVES IN PERSONAL CHANNELS

Personal email accounts, messaging apps, and social media feeds remain the most effective environments for phishing attacks. When these channels share devices or browsers with business systems, a single click can expose company data.

02 PASSWORD REUSE CREATES A DIRECT PATH

When credentials from a personal account are compromised, attackers routinely test them against business applications. This credential stuffing technique remains one of the easiest ways to gain unauthorized access.

03 RESTRICTIONS ALONE DON'T WORK

Blocking personal applications and enforcing strict policies often drives users toward workarounds. The risk doesn't disappear—it simply moves somewhere IT can no longer see.

WHAT ACTUALLY REDUCES RISK

Separate work and personal browsing environments, establish clear identity boundaries, and assume credentials will eventually be exposed somewhere. Layered security controls such as MFA and strong identity protection dramatically reduce the impact of stolen credentials.

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.

HOW PHISHING SITES STEAL YOUR ACTIVE LOGIN

Many businesses believe MFA alone protects their cloud accounts; however, while MFA remains essential, attackers are increasingly bypassing login credentials and instead targeting already authenticated sessions, where active session tokens can be stolen and reused.

ADVERSARY-IN-THE-MIDDLE (AITM) ATTACKS

LIVE PHISHING PROXIES

AiTM phishing sites act as reverse proxies between users and legitimate services. Users enter credentials, complete MFA, and unknowingly provide attackers with access to their active session.

SESSION COOKIE THEFT

After authentication, websites issue session tokens that prove a user has already logged in. Attackers steal these tokens and use them to access accounts without needing passwords or MFA.

WHAT HAPPENS NEXT

Once inside a trusted session, attackers can create hidden mailbox rules, register new MFA methods, monitor financial conversations, and launch phishing attacks from legitimate accounts.

MFA IS STILL ESSENTIAL, BUT IT'S NOT THE FINISH LINE

HOW "JUST-IN-TIME" ELEVATION HELPS YOUR TEAM

Permanent administrator privileges increase risk and reduce visibility.
With Just-in-Time (JIT) Elevation:

- Users receive temporary administrative access only when required.
- Every elevation request is logged and monitored.
- Access automatically expires when the approved task is complete.
- IT gains visibility without slowing productivity.

> *"The goal isn't removing productivity. It's removing unnecessary risk."*

PASSKEY MIGRATION CHECKLIST

- Audit which platforms already support passkeys
- Prioritize administrators and high-risk users
- Maintain passwords during a phased rollout
- Use password managers for unsupported systems
- Establish clear recovery and synchronization procedures
- Audit all SaaS applications connected to identity providers
- Cross-reference subscriptions with billing records
- Review HR termination records
- Remove public sharing permissions
- Audit Salesforce, Asana, Notion, and similar platforms
- Identify unmanaged AI and productivity tools
- Replace shared accounts with named users
- Review inactive accounts regularly
- Establish quarterly audits
- Enforce MFA on all remaining active accounts

PROTECTING ACCOUNTS PAYABLE FROM AI FRAUD

01 VERIFY PAYMENT REQUESTS THROUGH A SECOND CHANNEL
Always confirm payment or banking changes using a different communication method before acting.

02 DON'T TRUST APPEARANCES ALONE
Treat emails and messages as untrusted since AI can make them look completely legitimate.

03 REQUIRE EXTRA VERIFICATION FOR VOICE REQUESTS
Verify voice requests through another channel because AI can mimic real voices.

04 STANDARDIZE PAYMENT APPROVAL PROCEDURES
Use consistent approval steps to prevent mistakes and reduce fraud risk.

05 ENFORCE MFA AND ROLE-BASED ACCESS CONTROLS
Restrict access and use MFA to protect financial systems from unauthorized entry.

> *"Trust should be verified, especially when money is involved."*

TECHNOLOGY TRIVIA QUESTION

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

What video game was inspired by a pizza with one slice missing?

LAST MONTH'S ANSWER: **Radar**

Email info@hermescloud.nl to win!

amazon

$50 GIFT CARD