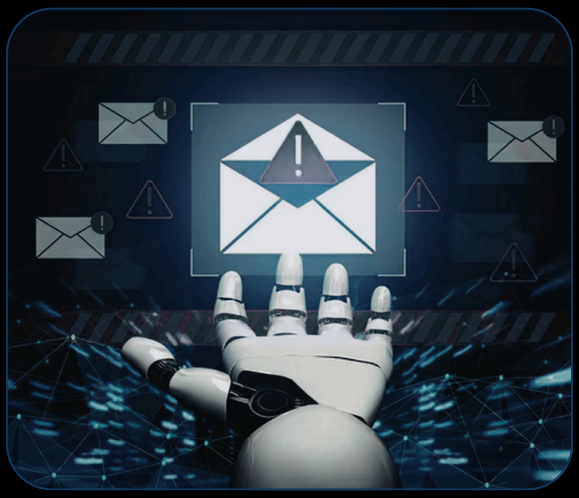
HERMES CLOUD
MANAGED IT SERVICES

VOLUME 006 • SEPTEMBER 2026
AMSTERDAM, THE NETHERLANDS

TECH TALK

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



INSIDE THIS ISSUE

How to Spot a Scam Email Now That They Look Real ----P1
Gadget of the Month ----P1
Is Your Website a Security Risk? ----P2
When Microsoft 365 Goes Down ----P2
Why Scroll Past the First Google Result? ----P2
OneDrive or SharePoint? ----P2
30-Minute IT Check ----P2
Technology Trivia ----P2

HOW TO SPOT A SCAM EMAIL NOW THAT THEY LOOK REAL

THE OLD "BAD SPELLING" TEST NO LONGER WORKS.

For years, the advice was simple: watch for bad spelling and clumsy grammar. Scammers now use AI to write their emails, so messages arriving in your team's inbox can read just like areal company's.

AI can produce convincing phishing without the translation, spelling and grammar mistakes that used to reveal it. Attackers can also feed public details about your company into an AI tool and get back the right names, job titles and a believable reason to be in touch.

Why these emails are convincing: the writing is clean, the message is personal, and there is a believable reason to contact you. AI also makes each message faster to produce, so attackers can send far more.

Your spam filter won't catch them all. A well-written, personalized email asking a normal-sounding question may carry no obvious bad link or attachment. The last line of defense is a person who knows what to check.

HOW SCAM EMAIL WORKS, AND HOW TO PREVENT THEM

01 LOOK AT WHAT IT ASKS YOU TO DO
Money, gift cards, a new account, a login, a code, personal details, or a surprising link or attachment.

02 WATCH FOR PRESSURE
Deadlines, threats, "do this now," or a request to change supplier bank details are all reasons to slow down.

03 VERIFY THE REAL PERSON
Display names can be copied. Use a phone number you already have—not one supplied by the message.

HOW TO PROTECT YOUR TEAM

Confirm payment changes by phone, use phishing-resistant MFA or passkeys, and make reporting suspicious email easy.



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.

IS YOUR BUSINESS WEBSITE A SECURITY RISK?

Your website is easy to set up and then forget. That is exactly why a neglected website is a common way a small business gets hacked. WordPress powers more than 40% of all websites; the risk is usually the plugins and themes added to it, which often go years without updates.

HOW IT HAPPENS

Automated tools scan huge numbers of sites for known weak spots. When a flaw is found, the plugin maker releases an update—but until it is installed, the hole stays open.

HOW TO KEEP IT SAFE

- Keep WordPress, plugins and themes updated.
- Remove plugins you do not use; stick to well-known, supported ones.
- Lock down the admin login with a strong, unique password and MFA.
- Add a reputable security plugin or firewall.
- Keep recent backups and decide clearly who owns website security.

WHY YOU SHOULD SCROLL PAST THE FIRST RESULT ON GOOGLE

Scammers buy ads on trusted names, so fake sites can sit above the real one.

- Scroll past sponsored results.
- Never download software from an ad.
- Bookmark sites you often use.
- Check the web address before entering a password.
- Keep browsers and devices updated.
- Tell your team that top results can be a trap.
- If someone clicks a bad link, change the password and check the device.

ONEDRIVE OR SHAREPOINT?

WHERE FILES SHOULD LIVE

OneDrive is personal space for drafts and work only you need. SharePoint is the team's space; files in a Teams channel are already in SharePoint.

1. Put team files in SharePoint or a Teams channel.
2. Keep OneDrive for your own drafts.
3. Move important files off local desktops.
4. Agree a simple rule so nobody has to guess.

When someone leaves, OneDrive is kept for only 30 days by default. Anything the team needs should be in SharePoint before that happens.

THE 30-MINUTE IT CHECK

Most owners look at IT only after something breaks. Verizon's 2026 DBIR found 31% of breaches started with software that had not been patched.

01 UPDATES
Check devices and software are not sitting at "restart required."

02 BACKUPS
Check when someone last restored a file. If it has never been tested, you do not know it works.

03 ACCESS & MFA
Every account should belong to an active employee and MFA should be on for everyone.

04 DEVICES & SUBSCRIPTIONS
Remove unknown devices and licenses for people who have left.

05 CALENDAR IT
Give the same person a fixed day each month and write down what they find.

TECHNOLOGY TRIVIA QUESTION

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

What does IMAX stand for?

LAST MONTH'S ANSWER:
Long Term Evolution

Email info@hermescloud.nl to win!

amazon

$50 GIFT CARD