How cyberattackers are targeting SMBs in Europe and Africa in 2025

Key attack vectors SMBs must understand to stay protected

kaspersky

kaspersky.com

Introduction

Cyberattackers often view small and medium-sized businesses (SMBs) as easier targets, assuming their security measures are less robust than those of larger enterprises. In fact, attacks through contractors, also known as trusted relationship attacks, remain one of the top three methods used to breach corporate networks. With SMBs generally being less protected than large enterprises, this makes them especially attractive to both opportunistic cybercriminals and sophisticated threat actors.

At the same time, AI-related attacks are becoming increasingly common, making phishing and malware campaigns easier to prepare and quickly adapt, thus increasing their scale. Meanwhile, cybersecurity regulations are tightening, adding more compliance pressure on SMBs.

Improving your security posture has never been more critical. Kaspersky highlights key attack vectors every SMB should be aware of to stay protected.

How malware and potentially unwanted applications (PUAs) are disguised as popular services

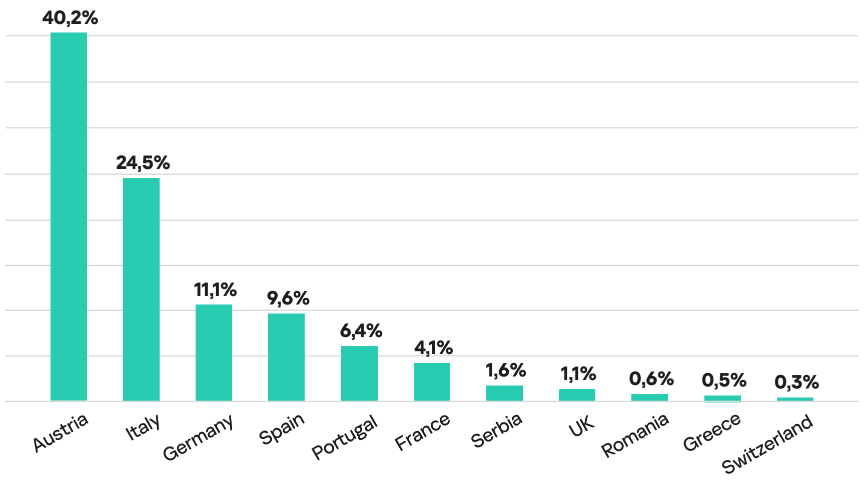
Kaspersky analysts have used data from the Kaspersky Security Network (KSN) to explore how frequently malicious and unwanted files and programs are disguised as legitimate applications commonly used by SMBs in Europe (UK, Italy, France, Germany, Spain, Portugal, Serbia, Greece, Romania, Austria and Switzerland) and select countries in North, West and Central Africa (Morocco, Tunisia, Algeria, Senegal, Cameroon and Ivory Coast). The KSN is a system for processing anonymized cyberthreat-related data shared voluntarily by opted-in Kaspersky users. For this research, only data received from the users of Kaspersky solutions for SMBs were analyzed. The research focused on the following applications:

- ChatGPT
- Cisco AnyConnect
- DeepSeek
- Google Drive
- Google Meet
- Microsoft Excel
- Microsoft Outlook
- Microsoft PowerPoint
- Microsoft Teams
- Microsoft Word
- Perplexity
- Salesforce
- Zoom

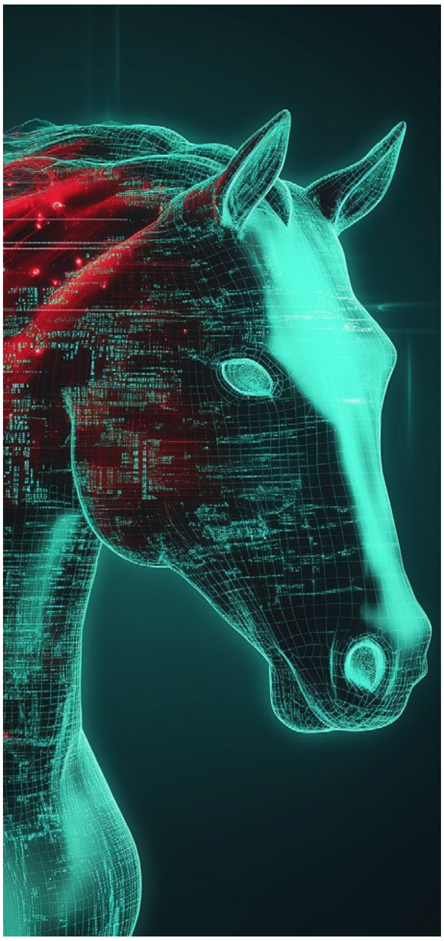
SMB threat landscape in Europe

In 2025, Austria accounted for the largest share of attacks targeting small and medium businesses among the analyzed European countries, making up 40.2% of all detected cases[1]. Italy followed with 24.5%, Germany with 11.1%, while Spain and Portugal saw shares of 9.6% and 6.4%, respectively. France contributed 4.1% of cases, and Serbia and the UK each held around 1%. Other countries, including Romania, Greece, and Switzerland, each represented less than 1% of the total share, indicating relatively low targeting activity.

Distribution of malware and PUA attacks mimicking legitimate applications on SMBs across selected European countries in 2025



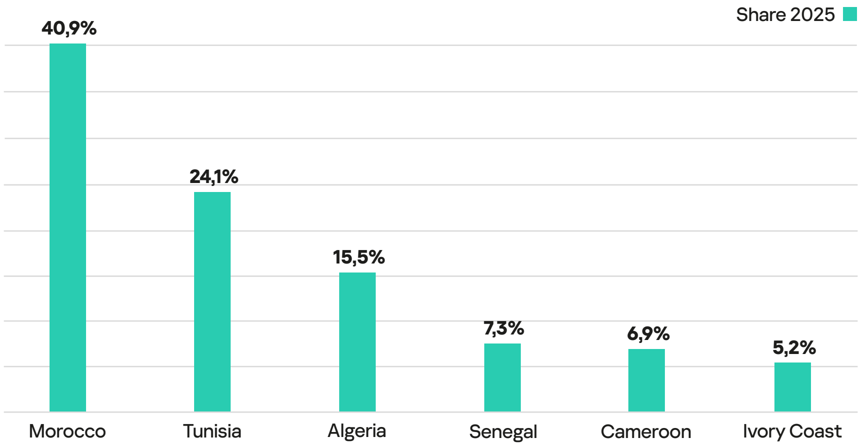
[1] The number of attacks in this report indicates how many times Kaspersky products for small and medium businesses detected malware or potentially unwanted applications (PUAs) mimicking legitimate brands from the analyzed sample



SMB threat landscape in parts of North, West and Central Africa

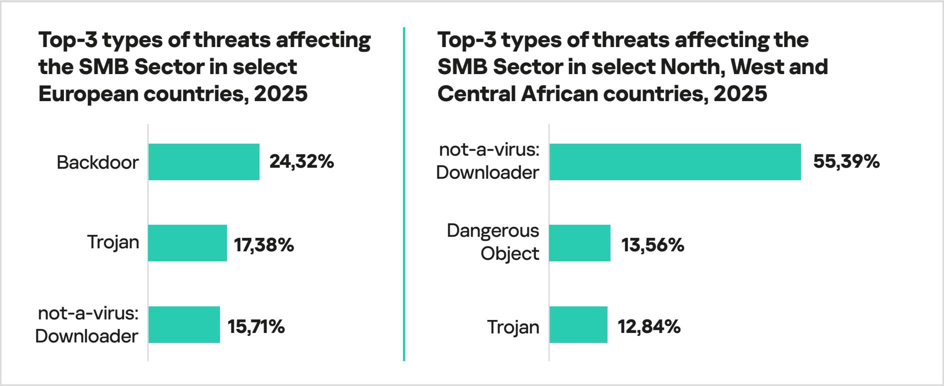
In 2025, Morocco accounted for the largest share of attacks among the analyzed African countries, making up 40.9% of all detected cases. Tunisia followed with 24.1%, while Algeria contributed 15.5%. Senegal and Ivory Coast saw more modest shares at 7.3% and 5.2%, respectively. Cameroon held a relatively small portion of 6.9%.

Distribution of malware and PUA attacks mimicking legitimate applications on SMBs across selected North, West and Central African countries in 2025



The top threats targeting small and medium businesses

The top threats targeting SMBs in select European countries included backdoor (24.32%), Trojan (17.38%) and not-a-virus:Downloader (15.71%). While in Africa not-a-virus:Downloader was the main type of threat (55.39%), followed by DangerousObject (13.56%) and Trojan (12.84%).


Top-3 types of threats affecting the SMB Sector in select European countries, 2025

Top-3 types of threats affecting the SMB Sector in select North, West and Central African countries, 2025

Backdoors provide cybercriminals with remote administration of a victim's machine. Unlike legitimate remote administration utilities, backdoors install, launch and run invisibly, without the consent or knowledge of the user. Once installed, backdoors can be instructed to send, receive, execute and delete files, harvest confidential data from the computer, log activity, and more.

Downloaders meanwhile are potentially unwanted applications designed to install additional content from the internet, often without clearly informing the user of what's being downloaded. While not inherently malicious, these tools are frequently exploited by attackers to deliver harmful payloads to victims' devices.

In Europe, Backdoors represented **24.32%** of SMB threats, while in Africa, not-a-virus Downloaders dominated with **55.39%**.

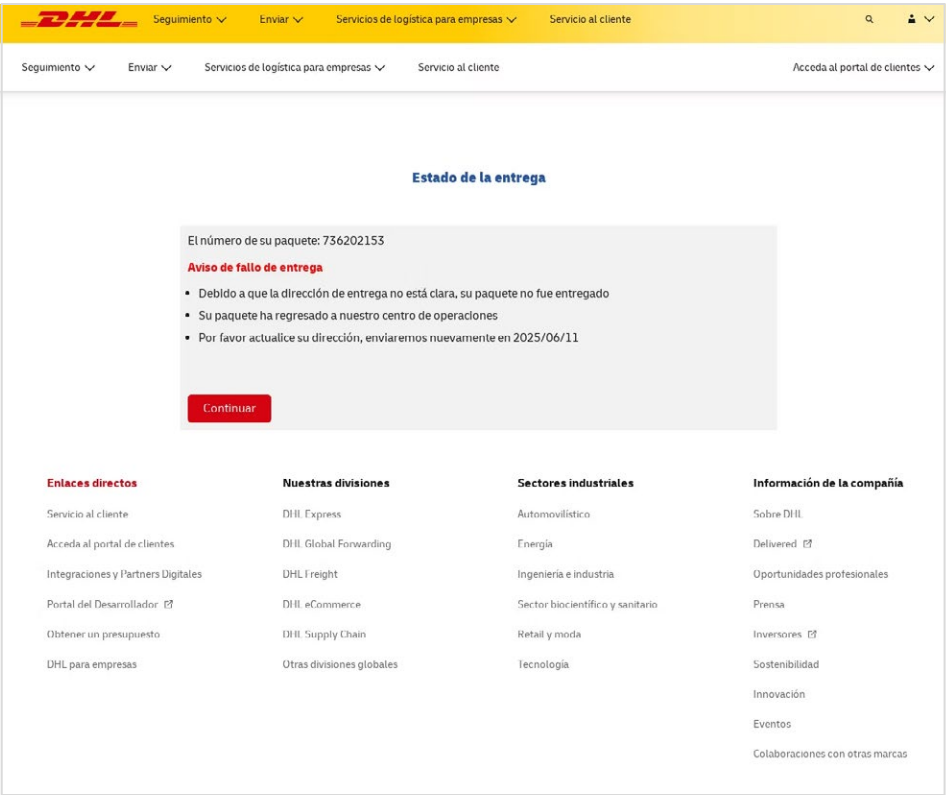
Trojans are malicious programs that carry out unauthorized actions such as deleting, blocking, modifying, or copying data, or disrupting the normal operation of computers and networks. Trojans are among the most prevalent forms of malware, and cyberattackers continue to use them in a wide range of malicious campaigns.

As for dangerous objects, they are malicious objects that, at the moment, do not have a precise classification. They may include various types of malwares like Trojans or adware, and other potentially unwanted or malicious files detected by Kaspersky's solutions.

How scammers and phishers trick victims into giving up accounts and money

We continue to observe a wide range of phishing campaigns and scams targeting SMBs. Attackers aim to steal login credentials for various services, from delivery platforms to banking systems, or manipulate victims into sending them money.

To do this, cyberattackers use a variety of lures, often imitating landing pages from brands commonly used by SMBs. One example is a convincing but fake page impersonating delivery company DHL, which attempts to lure victims into paying for a redelivery of a product. The scammers have taken great care to replicate the form DHL uses in cases where its drivers cannot deliver a product for any reason. For SMBs that receive multiple deliveries per day, where managers might not have visibility into every delivery, it can be easy to quickly sign off and pay small amounts for redelivery.


DHL
Seguimiento
Enviar
Servicios de logística para empresas
Servicio al cliente
Seguimiento
Enviar
Servicios de logística para empresas
Servicio al cliente
Acceda al portal de clientes

Estado de la entrega

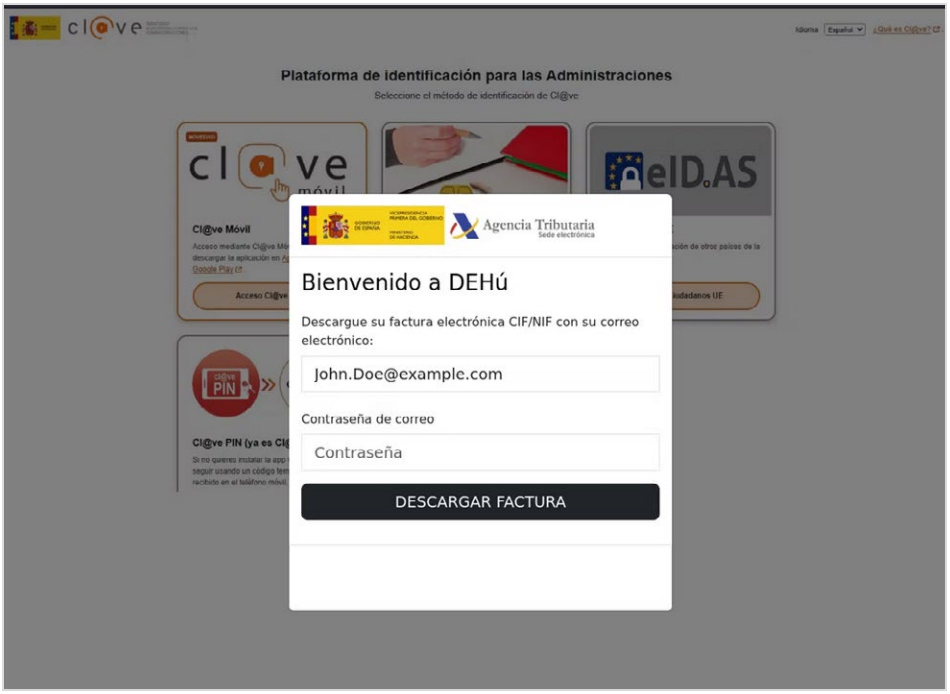
El número de su paquete: 736202153

Aviso de fallo de entrega

- Debido a que la dirección de entrega no está clara, su paquete no fue entregado
- Su paquete ha regresado a nuestro centro de operaciones
- Por favor actualice su dirección, enviaremos nuevamente en 2025/06/11

SMBs that receive multiple deliveries per day are particularly vulnerable, as they may not verify each one individually.

The phishing example below shows what appears to be the website of the Spanish tax authority, Agencia Tributaria, attempting to lure victims into sharing their credentials. Scammers use tactics like this where the sender has a reputation for being both highly trusted but also illegal to ignore to hurry victims into making rash decisions. Creating a sense of urgency for the victim is the key that unlocks this scam.



Plataforma de identificación para las Administraciones

Seleccione el método de identificación de Cl@ve

Cl@ve Móvil

Acceso mediante Cl@ve Mó… descargar la aplicación en A… Google Play

Cl@ve PIN (ya es Cl…

Si no quieres instalar la app … seguir usando un código tem… recibido en el teléfono móvil.

…ción de otros países de la

Bienvenido a DEHú

Descargue su factura electrónica CIF/NIF con su correo electrónico:

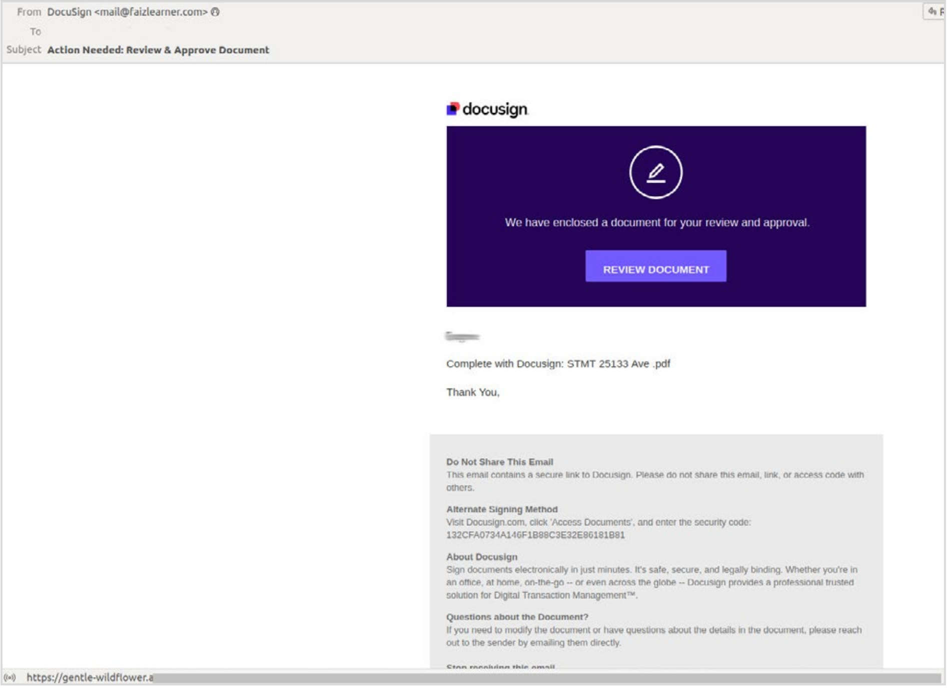
John.Doe@example.com

Contraseña de correo

Contraseña

DESCARGAR FACTURA

We also saw a range of phishing emails targeting SMBs. In one recent case detected by our systems, the attacker sent a fake notification allegedly from DocuSign, an electronic document-signing service.



From DocuSign <mail@faizlearner.com>

To

Subject **Action Needed: Review & Approve Document**

We have enclosed a document for your review and approval.

[redacted]

Complete with Docusign: STMT 25133 Ave .pdf

Thank You,

Do Not Share This Email

This email contains a secure link to Docusign. Please do not share this email, link, or access code with others.

Alternate Signing Method

Visit Docusign.com, click 'Access Documents', and enter the security code: 132CFA0734A146F1B88C3E32E86181B81

About Docusign

Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- Docusign provides a professional trusted solution for Digital Transaction Management™.

Questions about the Document?

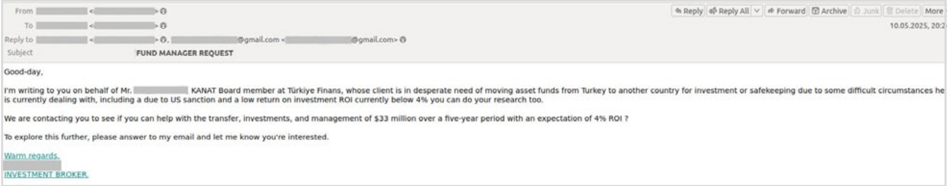
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly.

Stop receiving this email

https://gentle-wildflower.a

SMBs can even find themselves targeted by classic Nigerian scams. In one recent example, the sender claimed to represent a wealthy client from Turkey who wanted to move $33 million abroad to allegedly avoid sanctions, and invited the recipient to handle the funds. In Nigerian scams, fraudsters typically cajole money. They may later request a relatively small payment to a manager or lawyer compared to the amount originally promised.

> Security hardening maximizes protection by reducing the attack surface, keeping SMBs safe without extra costly solutions.



From [redacted] <[redacted]>
To [redacted] <[redacted]>
Reply to [redacted] <[redacted]>, [redacted]@gmail.com <[redacted]@gmail.com>
Subject FUND MANAGER REQUEST
10.05.2025, 20:2

Good-day,

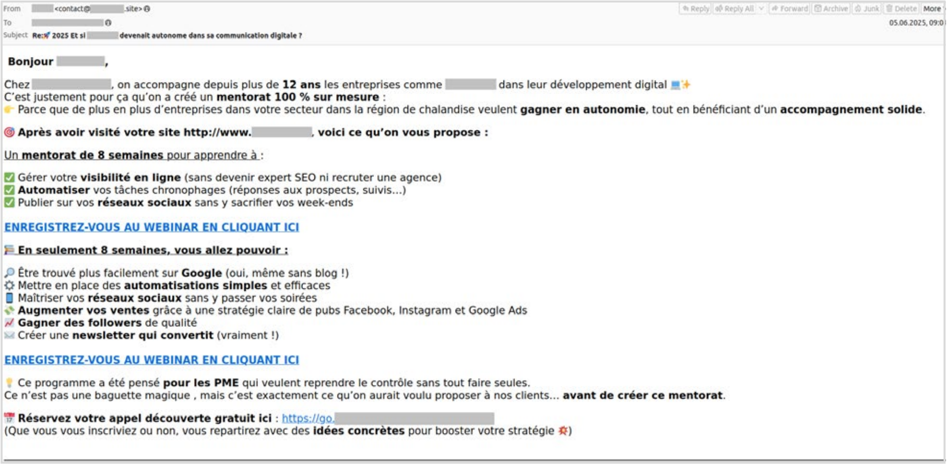
I'm writing to you on behalf of Mr. [redacted] KANAT Board member at Türkiye Finans, whose client is in desperate need of moving asset funds from Turkey to another country for investment or safekeeping due to some difficult circumstances he is currently dealing with, including a due to US sanction and a low return on investment ROI currently below 4% you can do your research too.

We are contacting you to see if you can help with the transfer, investments, and management of $33 million over a five-year period with an expectation of 4% ROI ?

To explore this further, please answer to my email and let me know you're interested.

Warm regards,
[redacted]
INVESTMENT BROKER.

Beyond these threats, SMBs are bombarded daily with hundreds of spam emails. Some promise attractive deals on email marketing or loans; others offer services like reputation management, content creation, or lead generation. In general, these offers are crafted to reflect the typical needs of small businesses.



From [redacted] <contact@[redacted].site>
To [redacted]
Subject Re:🚀 2025 Et si [redacted] devenait autonome dans sa communication digitale ?
05.06.2025, 09:0

Bonjour [redacted]**,**

Chez [redacted], on accompagne depuis plus de **12 ans** les entreprises comme [redacted] dans leur développement digital 💻✨
C'est justement pour ça qu'on a créé un **mentorat 100 % sur mesure** :
👉 Parce que de plus en plus d'entreprises dans votre secteur dans la région de chalandise veulent **gagner en autonomie**, tout en bénéficiant d'un **accompagnement solide**.

🎯 **Après avoir visité votre site http://www.**[redacted]**, voici ce qu'on vous propose :**

Un **mentorat de 8 semaines** pour apprendre à :

✅ Gérer votre **visibilité en ligne** (sans devenir expert SEO ni recruter une agence)
✅ **Automatiser** vos tâches chronophages (réponses aux prospects, suivis...)
✅ Publier sur vos **réseaux sociaux** sans y sacrifier vos week-ends

ENREGISTREZ-VOUS AU WEBINAR EN CLIQUANT ICI

🏁 **En seulement 8 semaines, vous allez pouvoir :**

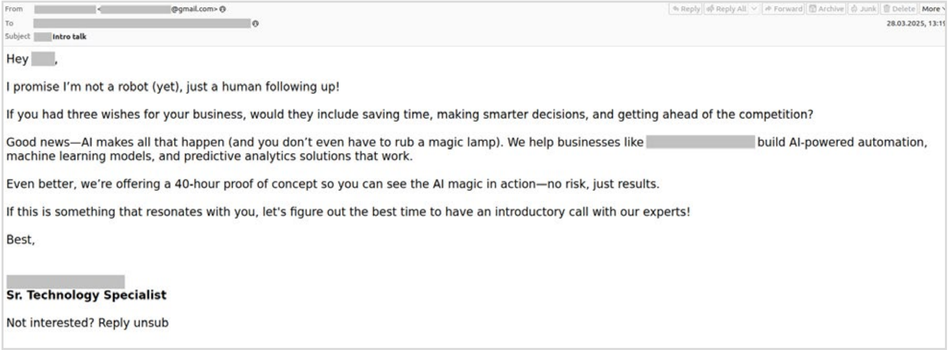
🔎 Être trouvé plus facilement sur **Google** (oui, même sans blog !)
⚙ Mettre en place des **automatisations simples** et efficaces
📱 Maîtriser vos **réseaux sociaux** sans y passer vos soirées
💸 **Augmenter vos ventes** grâce à une stratégie claire de pubs Facebook, Instagram et Google Ads
📈 **Gagner des followers** de qualité
✉ Créer une **newsletter qui convertit** (vraiment !)

ENREGISTREZ-VOUS AU WEBINAR EN CLIQUANT ICI

💡 Ce programme a été pensé **pour les PME** qui veulent reprendre le contrôle sans tout faire seules.
Ce n'est pas une baguette magique , mais c'est exactement ce qu'on aurait voulu proposer à nos clients... **avant de créer ce mentorat**.

📅 **Réservez votre appel découverte gratuit ici** : https://go.[redacted]
(Que vous vous inscriviez ou non, vous repartirez avec des **idées concrètes** pour booster votre stratégie 💥)

Not surprisingly, AI has also made its way into the spam folder – with offers to automate various business processes.



From [redacted] <[redacted]@gmail.com>
To [redacted]
Subject [redacted] Intro talk
28.03.2025, 13:1

Hey [redacted],

I promise I'm not a robot (yet), just a human following up!

If you had three wishes for your business, would they include saving time, making smarter decisions, and getting ahead of the competition?

Good news—AI makes all that happen (and you don't even have to rub a magic lamp). We help businesses like [redacted] build AI-powered automation, machine learning models, and predictive analytics solutions that work.

Even better, we're offering a 40-hour proof of concept so you can see the AI magic in action—no risk, just results.

If this is something that resonates with you, let's figure out the best time to have an introductory call with our experts!

Best,

[redacted]
Sr. Technology Specialist

Not interested? Reply unsub

Security tips

SMBs can reduce risks and ensure business continuity by investing in comprehensive cybersecurity solutions and increasing employee awareness. It is essential to implement robust measures such as spam filters, email authentication protocols, and strict verification procedures for financial transactions and the handling of sensitive information.

Another key step toward cyber resilience is promoting awareness about the importance of comprehensive security procedures and ensuring they are regularly updated. Regular security training sessions, strong password practices, and multi-factor authentication can significantly reduce the risk of phishing and fraud.

It is also worth noting that searching for software through search engines is an insecure practice, and should be prohibited in the organization. If you need to implement new tools or replace existing ones, make sure they are downloaded from official sources and installed on a centralized basis by your IT team.

Security hardening: a cost-effective strategy for resource-bounded organizations

Attackers can use not only phishing and social engineering techniques to breach organizations, but also many other potential points of entry, such as unpatched vulnerabilities or default credentials, collectively known as the attack surface in professional terms. To minimize the risk of successful attacks, it is advisable to implement security hardening – techniques and procedures to protect infrastructure by reducing an attack surface. Essentially, this involves turning the security of existing systems up to the maximum without resorting to extra protection solutions. The basic hardening recommendations include:

- Implementing strong authentication and authorization. This requires the enforcement of a strict password policy, the use of two-factor authentication and the implementation of network access control measures to reduce the risks of an unauthorized access to a company's systems and data.
- Regularly updating software and timely patching vulnerabilities. Regular updates of operation system, applications and other software will help prevent the risk of known vulnerability exploitation by cybercriminals.
- Encrypting data. Encryption of data at rest (when data is stored) as well as in transit (when data is moving between devices), protects them from interception and unauthorized access.
- Doing backups and data backups. A continuous backup process will reduce the risks of a destruction of data and business disruptions in case of a potential cyberattack, enabling companies to facilitate cyberattack remediation in case it happened.
- Training employees. A systematic approach to cyber education, carrying out regular assessments of the level of cyber literacy among staff and implementing the training that would fill gaps in employees' knowledge will help minimize the risks of attacks caused by a human factor.

For further information about Kaspersky Next, please visit kaspersky.com/next

Cybersecurity Action Plan for SMB

1. Consider **implementing hardening practices** described above to minimize the risk of successful attacks.
2. On top of that, **define access rules for corporate resources** such as email accounts, shared folders, and online documents. Monitor and limit the number of individuals with access to critical company data. Keep access lists up to date and revoke access promptly when employees leave the company. Use cloud access security brokers to monitor and control employee activities within cloud services and enforce security policies.
3. **Establish clear guidelines for using external services and resources**. Create well-defined procedures for coordinating specific tasks, such as implementing new software, with the IT department and other responsible managers. Develop short, easy-to-understand cybersecurity guidelines for employees, with a special focus on account and password management, email protection, and safe web browsing. A well-rounded training program will equip employees with the knowledge they need and the ability to apply it in practice.
4. **Implement specialized security solutions** such as Kaspersky Next that combine strong endpoint protection with EDR and XDR capabilities and are designed to benefit corporate customers of any size and industry. Especially Kaspersky Next XDR Optimum is suitable for SMBs with an established IT infrastructure, which are often managed by larger IT teams or small security units. For very small businesses that may not have an IT administrator, Kaspersky Small Office Security (KSOS) offers hands-off protection through its “install and forget” setup.

News about cyber threats: securelist.com/
IT security news: kaspersky.com/blog/
IT security for SMBs: kaspersky.com/small-to-medium-business-security

kaspersky

kaspersky.com