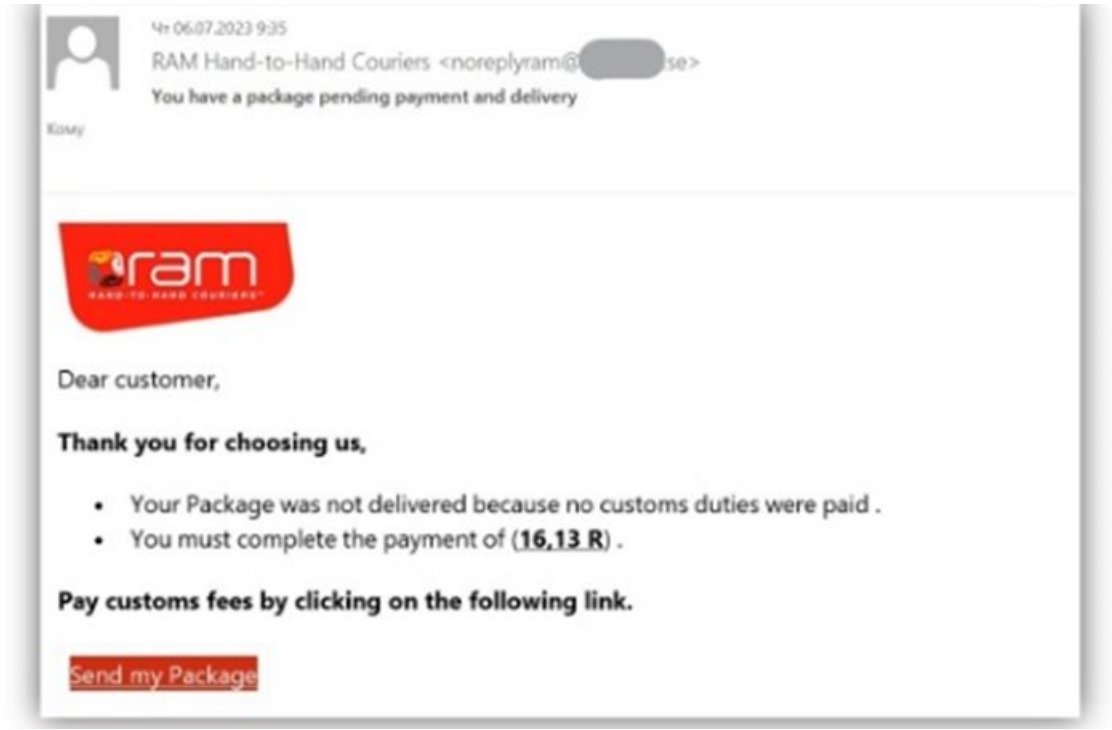
Beware: courier package undelivered email scam on the rise

Kaspersky experts have detected a rise in scams where fraudsters are posing as RAM couriers to trick unsuspecting users into sharing bank account information by claiming packages were undelivered due to unpaid customs fees. To date there have been no emails claiming to be other popular courier services.

Scam alert: fraudsters posing as courier companies. Source: Brett Jordan/Unsplash

Cybercriminals are sending deceptive emails that appear to be from RAM courier service, falsely claiming that a package was not delivered due to pending customs fees. To create a sense of urgency, the email urges users to click on a provided link for further instructions.

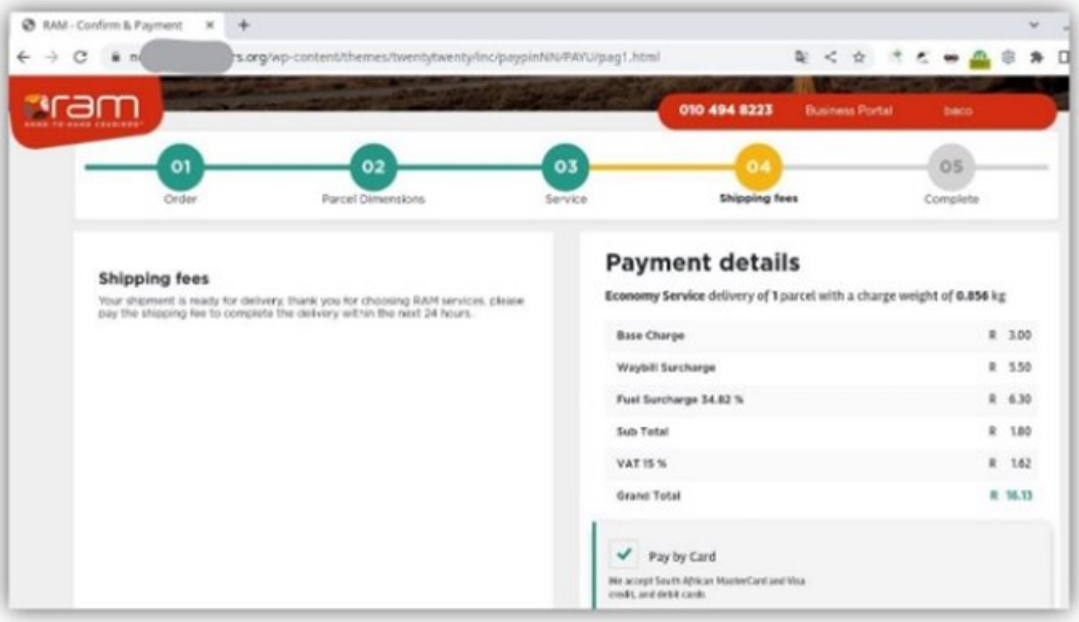


Fraudulent email example detected by Kaspersky.

When users click on the link, they are redirected to a fraudulent website masquerading as a legitimate RAM courier service

portal.

Upon reaching the fraudulent website, victims are prompted to input their bank card credentials, providing cybercriminals with direct access to sensitive financial information. Falling prey to this scam exposes individuals to potential identity theft, financial fraud, and significant personal losses.

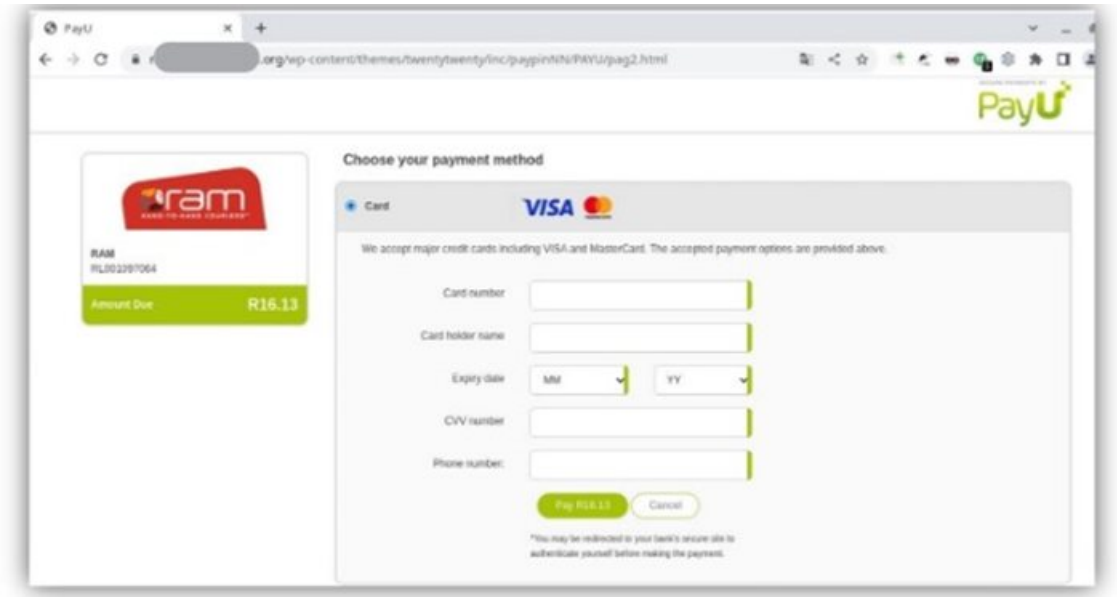


Fake RAM website asking for payment of shipping fees.

It’s important to note that the website and the email domains used by the scammers have no relation to RAM and are clearly fake.

“As technology continues to permeate all aspects of our lives, the use of courier services continues to grow and plays an important logistics role, especially for the eCommerce market," says Roman Dedenok, spam analysis expert at Kaspersky.

In South Africa the courier, express and parcel (CEP) market revenue is expected to grow from R44bn in 2022 to R60bn by 2027.



Users are asked for their bank card details.

"The sad reality is that cybercriminals see this as an opportunity to exploit the market and customers using such services on a regular basis, trying to trick them with scam and phishing mails. And although our research has identified specific tactics using the RAM name, it should be noted that such scams do also use the names of other popular courier services and come in the form of SMS too, and not just email," Dedenok continues.

"When watching out for scam and phishing emails, pay attention to the emotional tone conveyed in the message. Scammers often try to evoke fear, excitement, or urgency, to manipulate recipients into taking impulsive actions. Take a step back and analyse how the email makes you feel. This can be key to identifying and avoiding phishing scams effectively."

Scam alert: Unlawful activity under the alias 'So Interactive'

So Interactive 1 Aug 2023

Online safety

Try these tips to stay safe and not fall victim to phishing:

Verify website authenticity: Before making any transactions or providing personal details, double-check the website's URL for secure connections (look for "https" and a padlock icon). Be wary of websites with slight misspellings or unusual domain names, as these may indicate fraudulent activity.

Pay careful attention: Before clicking on any links received in an email or via an SMS message, as these could be potential phishing links.

Invest in security: For businesses, implement protection at the mail gateway level to lessen the likelihood of corporate employees encountering phishing emails. Internet-facing devices need to be protected by an endpoint security solution.

Develop a culture of awareness: Hold regular awareness training for employees on the latest cyberthreats, or, at the very least, regularly inform them of potential phishing scams.