# PEC “invoice scam” - Stealing time, money, and trust from businesses

Archived: 2026-04-05 12:47:08 UTC

## Introduction

## A brief introduction to PEC

The service enables senders to prove that an email has been sent and received from one PEC mailbox to another PEC mailbox, in a court of law. It is often used to send important documents to public administration, citizens, and private companies. Because the emails are legally binding, it means the recipient cannot reject the mail - or claim to have not received it.

## PEC is a trusted service, isn’t it?

According to official AgID data, in 2022 there were approximately 15 million active PEC email boxes in Italy, and more than 2.5 billion messages were exchanged - making it a highly valued, effective and trusted tool. Inspired by its success, the European Commission is pushing for adoption of REM (Registered Electronic Email) across the EU - an initiative intended to standardize and address the lack of interoperability among digital certified email services within the EU. At face value, this absolutely makes sense.

However, malicious actors are *already* using PEC to send emails, leveraging its features to target everyday people. With an interconnected “European PEC” that expands throughout Europe, criminals will have an infinitely greater opportunity to exploit certified email.

## How can businesses protect their PEC mailbox?

Considering the potential scope of the so-called “European PEC”, the pool of potential victims is set to grow exponentially. So, how can business owners protect their mailboxes? Here’s a quick five-step checklist to help minimize your risk:

- Configure your mailbox to accept messages only from other PEC mailboxes. While this won't prevent the case we'll be discussing, it will help reduce spam.
- Use a strong, unique password and enable two-factor authentication (where possible).
- Avoid sharing your login details…with anyone.
- Always check the "from" address of emails received.
- Don't click suspicious links, hover over them, instead. If they don’t make sense, that’s an immediate red flag.
- Before taking any action, always verify the email with the sender.

Having learned the basics of how to protect your business from PEC email abuse, let's take a closer look at the scam.

## The PEC “invoice scam”

As a self-confessed petrol head I’ve been following the YouTube channel, “GASI Garage,” for years. Ready for my latest installment of fumes and burnt rubber, I was shocked to hear Gabriele, talking about PEC, spam and scams ….apparently your job never leaves you alone!

In short, someone’s PEC credentials had been stolen, and used to send malspam to hundreds of other PEC addresses, including that of Gabriele. Here’s the email he received:

*Good morning GASI Automobiles, We’d like to inform you that, based on the contract you signed on 25/11, you must pay me 142 eur. However, that amount has not yet been paid despite numerous solicitation emails. If you don’t pay in 5 days, I’ll be obliged to contact my attorney for further legal actions. This is a formal warning and stops any prescription. You can download the Invoice by clicking the link “Invoice” (underlined!) Best Regards,*

Here we have a typical, "you need to pay this invoice - download here" email, where "here" is a link to some sort of malware or phish.

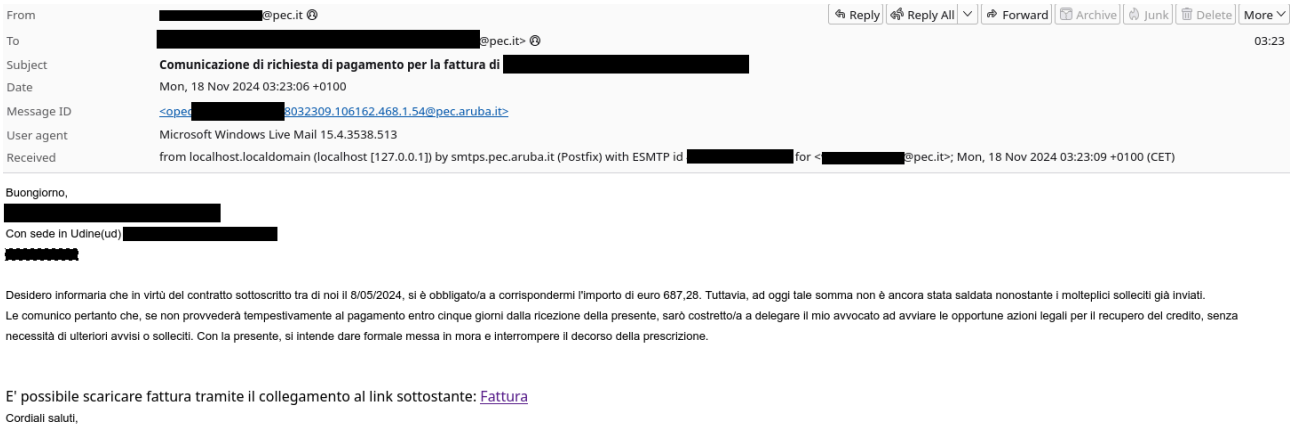
Because PEC is a legally binding email, Gabriele couldn’t simply ignore it, especially - as he admitted - he isn’t tech-savvy. As a result, this triggered a chain of verifications, including:

- Determining if and where he had spent the money
- Reviewing his incoming invoices
- Asking his accountant to check his invoices
- Contacting the certified sender (since it couldn’t be faked) for clarification

This wasted a considerable amount of time and hundreds of euros on Gabriele's side alone. When he finally reached the owner of the PEC email address, he was the 100th person to contact him. This suggests that countless others likely spent valuable working hours conducting the same checks. Additionally, the PEC sender had to repeatedly explain to everyone that the issue wasn’t directly his fault, further adding to the wasted time and aggravation. In the end, it collectively cost thousands of Euros and hours.

## Not the same campaign, again?

Yes, that's right! While I was working out at the gym, the owner approached me with a suspicious email, knowing my line of work. At first glance, I couldn't believe it, it was the exact same email campaign - only this time with a fresh malware sample ready for analysis!




## What do we know about the malware?

Spamhaus Malware Labs determined that the malicious link in the email triggers the download of a VBScript file, which results in the download of MintsLoader malware. This malware acts as a dropper, facilitating the delivery and installation of additional malware, such as credential stealers, RATs, or other malicious payloads. The likely outcome? Passwords will be exfiltrated and potentially exploited for malicious activities.

## And, what happened to the victims?

Luckily, there were no severe repercussions for the two victims highlighted here. They were savvy enough to detect the threat and take appropriate actions to verify. However, in the life of a mechanic, a gym owner, or any other business, wasted time means wasted money. Spam and malicious emails aren't just technical issues, they have real-life consequences.

## PEC mailbox providers: are they taking any action?

The PEC regulations typically allow for viruses and malware to be rejected, but not all forms of unsolicited messages (spam) can be outright rejected. Unfortunately, providers handling PEC mailboxes tend to apply minimal security measures, like scanning attachments for viruses, the use of stricter measures (e.g., using real-time blocklists or spam filters) risk legal complications.

Even moving PEC emails to the spam folder is rare, as explained by a court case where a misplaced email ended up in the spam folder. In this case, the court ruled the recipient was responsible for checking the spam folder.

Because of situations like this, operators have little incentive to provide anything above the minimum security for PEC mailboxes. As a result, business owners like Gabriele are more likely to receive spam, scams, and other malicious emails into their trusted PEC mailboxes.

If you receive a suspicious email, please follow the advice in this blog, report it to your PEC provider, and share it with Spamhaus' Threat Intel community portal to help protect others.

## Help and recommended content

See below for helpful articles and recommended content

---