“Hello pervert” sextortion scam includes new threat of Pegasus—and a picture of your home

By Pieter Arntz

Published: 2024-09-04 · Archived: 2026-04-05 22:05:53 UTC

After using passwords obtained from one of the countless breaches as a lure to trick victims into paying, the “Hello pervert” sextortion scammers have recently introduced two new pressure tactics: Name-dropping the infamous Pegasus spyware and adding pictures of your home environment.

They do this to add credibility to the false claims that the scammers have been watching your online behavior and caught you red-handed during activities that you would like to keep private amongst your friends and family.

The email usually starts with “Hello pervert” and then goes on to claim that the target has been watching pornographic content. The scammers often claim to have footage of what you were watching and what you were doing while watching.

To stop the sender from spreading the incriminating footage, the target will have to pay the scammer, or else they will send it to everyone in their email contacts list.

More recently, scammers have started increasing their threats by mentioning a powerful spyware called “Pegasus.” Several versions of these scam emails have included the following text:

> Have you heard of Pegasus? This is a spyware program that installs on computers and smartphones and allows hackers to monitor the activity of device owners. It provides access to your webcam, messengers, emails, call records, etc. It works well on Android, iOS, and Windows.

Though Pegasus is indeed a powerfully invasive spyware tool, the threat of its use, as included in these scam emails, is entirely empty. This is because Pegasus has never been observed outside of a surveillance campaign carried out, specifically, by governments. Time and time again, Pegasus has been used by oppressive government regimes to spy on political dissidents, human rights activists, and watchdog journalists. There is essentially no proof that such a closely-guarded spyware has ended up in the hands of everyday scammers.

But the pressure tactics don’t end with Pegasus, as many of these emails include an old (or active) password that a scam target has used in the past. Here, this isn’t some act of advanced hacking. Instead, it is likely that the scammers bought your password from other cybercriminals that obtained them during one of the countless data breaches that hit company after company every week.

When scammers have access to such data, it may also include your physical address. With that knowledge, scammers have increased their threats by simply adding a photograph of your personal neighborhood by looking it up online. For most places in inhabited areas, you can grab such pictures from Google Maps or similar apps.

A Reddit user demonstrated this by finding that such a scammer used an old PO box address. But it's true that this adds a convincing argument to the claim that the sender has been spying on you.

As an extra threat the email may include something like:

> "Or is visiting [your physical address] a more convenient way to contact if you don't take action. Nice location btw."

Implying that they know where you live and threatening to stop by and create a scene.

How to recognize "Hello pervert" emails

Once you know what's going on it's easy to recognize these emails. Remember that not all of the below characteristics have to be included in these emails, but all of them are red flags in their own right.

- They often look as if they came from one of your own email addresses.
- The scammer accuses you of inappropriate behavior and claims to have footage of that behavior.
- In the email the scammer claims to have used Pegasus or some Trojan to spy on you through your own computer.
- The scammer says they know "your password."
- You are urged to pay up quickly or the so-called footage will be spread to all your contacts. Often you're only allowed one day to pay.
- The actual message often arrives as an image or a pdf attachment. Scammers do this to bypass phishing filters.

How to react to "Hello pervert" emails

First and foremost, never reply to emails of this kind. It may tell the sender that someone is reading the emails sent to that address and they will repeatedly try new and other methods to defraud you.

- If the email included a password, make sure you are not using it any more and if you are, change it as soon as possible.
- If you are having trouble organizing your password, have a look at a password manager.
- Don't let yourself get rushed into action or decisions. Scammers rely on the fact that you will not take the time to think this through and subsequently make mistakes.
- Do not open unsolicited attachments. Especially when the sender address is suspicious or even your own.
- For your ease of mind, turn of your webcam or buy a webcam cover so you can cover it when you're not using the webcam.

Check your digital footprint

If you want to find out what personal data of yours has been exposed online, you can use our free Digital Footprint scan. Fill in the email address you're curious about (it's best to submit the one you most frequently use) and we'll send you a free report.

We don’t just report on threats—we help safeguard your entire digital identity

Cybersecurity risks should never spread beyond a headline. Protect your, and your family’s, personal information by using identity protection.

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.
