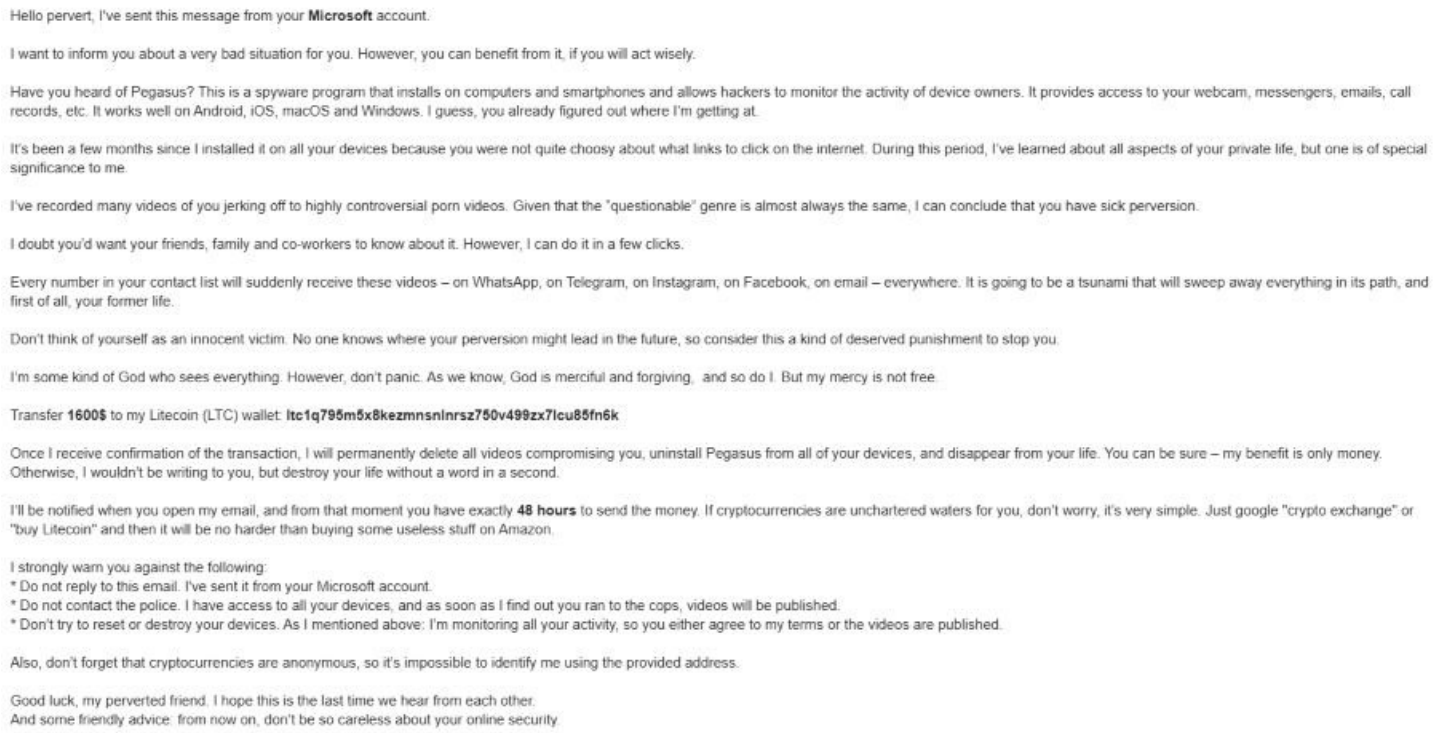
Ayer, me llegó un correo electrónico muy inquietante porque **aparentemente era enviado desde mi propia cuenta de Outlook**. Ya sabes que en mi haber, tengo decenas de emails de distintos servidores para diferentes usos. El mensaje decía que habían tomado el control de todos mis dispositivos, instalado un spyware llamado *Pegasus* y grabado videos comprometedores. ¿La solución que ofrecían? Enviar $1600 en criptomonedas para que no los difundieran por WhatsApp, Telegram, email y hasta Facebook.



Hello pervert, I've sent this message from your **Microsoft** account.

I want to inform you about a very bad situation for you. However, you can benefit from it, if you will act wisely.

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, macOS and Windows. I guess, you already figured out where I'm getting at.

It's been a few months since I installed it on all your devices because you were not quite choosy about what links to click on the internet. During this period, I've learned about all aspects of your private life, but one is of special significance to me.

I've recorded many videos of you jerking off to highly controversial porn videos. Given that the "questionable" genre is almost always the same, I can conclude that you have sick perversion.

I doubt you'd want your friends, family and co-workers to know about it. However, I can do it in a few clicks.

Every number in your contact list will suddenly receive these videos – on WhatsApp, on Telegram, on Instagram, on Facebook, on email – everywhere. It is going to be a tsunami that will sweep away everything in its path, and first of all, your former life.

Don't think of yourself as an innocent victim. No one knows where your perversion might lead in the future, so consider this a kind of deserved punishment to stop you.

I'm some kind of God who sees everything. However, don't panic. As we know, God is merciful and forgiving, and so do I. But my mercy is not free.

Transfer **1600$** to my Litecoin (LTC) wallet: **ltc1q795m5x8kezmnsnlnrsz750v499zx7lcu85fn6k**

Once I receive confirmation of the transaction, I will permanently delete all videos compromising you, uninstall Pegasus from all of your devices, and disappear from your life. You can be sure – my benefit is only money. Otherwise, I wouldn't be writing to you, but destroy your life without a word in a second.

I'll be notified when you open my email, and from that moment you have exactly **48 hours** to send the money. If cryptocurrencies are unchartered waters for you, don't worry, it's very simple. Just google "crypto exchange" or "buy Litecoin" and then it will be no harder than buying some useless stuff on Amazon.

I strongly warn you against the following:
* Do not reply to this email. I've sent it from your Microsoft account.
* Do not contact the police. I have access to all your devices, and as soon as I find out you ran to the cops, videos will be published.
* Don't try to reset or destroy your devices. As I mentioned above: I'm monitoring all your activity, so you either agree to my terms or the videos are published.

Also, don't forget that cryptocurrencies are anonymous, so it's impossible to identify me using the provided address.

Good luck, my perverted friend. I hope this is the last time we hear from each other.
And some friendly advice: from now on, don't be so careless about your online security.

¿Te suena a película? **Lo es. Pero también es un tipo de estafa muy real y peligrosa.**

¿Qué hacen estos delincuentes?

Utilizan una técnica llamada **spoofing** para hacerte creer que te escriben desde tu propia cuenta. Pero **no la hackearon**. Solo falsifican el remitente y usan un mensaje amenazante para generarte miedo y urgencia.

¿Cómo lo detecté?

1. **El correo no proviene realmente de Outlook.** La IP de origen (31.41.38.12) corresponde a un servidor desconocido, no a Microsoft.
2. **No pasó los controles de seguridad** (SPF, DKIM, DMARC), que son como los porteros digitales del correo. Los tres fallaron.
3. **El mensaje es genérico**, se envía a miles de personas con texto similar. Solo cambian el remitente para que parezca que te lo enviaste a ti mismo.
4. **No hay ninguna evidencia real** de lo que dicen. Es solo un intento de extorsión emocional.
5. Y por último, ya soy grande para esas «prácticas»....

¿Qué debés hacer si recibís algo así?

No respondas.

 No pagues nada (obvio!).
 Cambiá tu contraseña si tenés dudas.
 Activá la verificación en dos pasos.
 Marcá el correo como **phishing** en Outlook, Gmail o donde lo recibas.

Yo también decidí hacer mi parte

Apenas recibí este correo, además de analizarlo, decidí **reportarlo a una organización internacional llamada APWG (Anti-Phishing Working Group)**. ¿Por qué lo hice? Porque creo que si cada uno de nosotros denuncia este tipo de engaños, **contribuimos a una Internet más segura para todos**.

Lo reenvié directamente a **reportphishing@apwg.org**, pero también se puede hacer desde su web oficial:
 https://apwg.org/reportphishing/

Ellos se encargan de recopilar estos intentos de fraude, los analizan y colaboran con empresas y autoridades para tomar acciones. Es algo simple de hacer, y si más personas lo hacen, ayudamos a evitar que otros caigan en la trampa.

Te invito a que vos también lo hagas si alguna vez recibís algo sospechoso. No sólo te cuidás vos, sino que cuidás a otros que quizás no sabrían cómo actuar.

Como siempre, desde el Guía Tecnológico:

Estoy para ayudarte a detectar estos engaños, proteger tu privacidad y navegar tranquilo en el mundo digital. Este tipo de estafas crecen cada día y afectan especialmente a quienes no están familiarizados con los trucos modernos.
Nos seguimos cuidando entre todos.

Y recordá…

Yo soy Pablo, tu asistente tecnológico humano, como la IA, pero con «tracción a sangre».

Por favor, síguenos y danos «me gusta»:

Seguir
Compartir
Tuitear