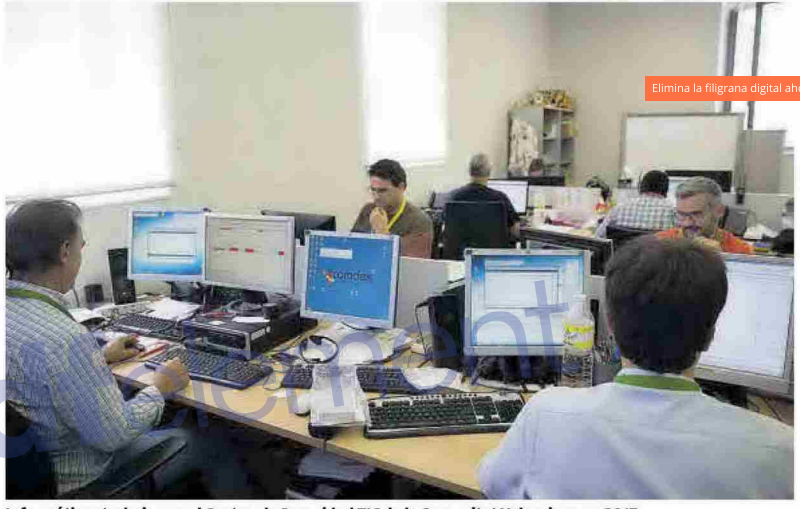
Nuevo caso de ciberataque con correos falsos en la universidad

▶ La UV avisa a su personal laboral de una campaña de mensajes fraudulentos que extorsionan por un vídeo sexual



Informáticos trabajan en el Centro de Seguridad TIC de la Comunitat Valenciana en 2017. F. BUSTAMANTE

Elimina la filigrana digital ahora

DIEGO AITOR SAN JOSÉ. VALÈNCIA

■ Le ha tocado una herencia. Tiene un paquete bloqueado en Correos. Pulse para recibir un pack de mascarillas de promoción. Evite que sus familiares se contagien de coronavirus. O la última: tenemos un vídeo sexual íntimo suyo. Son mensajes llegados por correo electrónico a direcciones de docentes de las universidades públicas valencianas con una cosa en común: todos son fraudulentos.

La última en advertir de ellos ha sido la Universitat de València. «Se ha detectado una nueva campaña de correos electrónicos fraudulentos», indica el correo interno a su personal laboral. «El objetivo es extorsionar a los destinatarios con el envío a sus contactos de un supuesto vídeo íntimo con contenido sexual o con la infección de covid-19 a sus familiares». En los dos casos, se amenaza con «hacer efectiva su extorsión si no se realiza el pago de dinero».

Un caso habitual

Ese tipo de avisos se ha convertido en un habitual en los últimos tiempos entre instituciones públicas y grandes empresas. «Todos los meses nos llegan este tipo de mensajes», indican desde la UV. Según indican, cuando se dan este tipo de campañas el servicio informático interno de la UV las detecta y envía un correo masificado al personal laboral informando de ello: «El hecho de que los ciberdelincuentes utilizan la dirección de correo electrónico UV, no implica que hayan entrado en las cuentas ni en los buzones».

Este problema no queda limitado exclusivamente a la Universitat de València. En la Universitat Politècnica de València, también aseguran que desde finales de diciembre están llegando correos fraudulentos. Explican que su objetivo es distribuir el malware Emotet, un programa malicioso que se intenta esparcir por todos los servidores posibles para troyanizar y tomar el control de estos.

Según desgranan desde la Politècnica, estos correos parece que provengan de un contacto conocido, «tienen un asunto y/o cuerpo del mensaje de conversaciones anteriores del destinatario», incluyen un adjunto que suele ser el malware que se distribuye en ese reenvío masivo.

Sin embargo, desde la UPV aseguran estar protegidos ya que el antivirus corporativo «detecta y bloquea todas las variantes del malware que se han recibido , con lo que los equipos protegidos con esta herramienta están a salvo».