

C07/CONV/2024 – ALERTAS DE CIBERSEGURIDAD

binauramonlex

Comunicamos las últimas alertas más destacadas a tener en cuenta por las empresas:

1. Si has usado ChatGPT, tus datos están en peligro; han robado más de 200.000 credenciales <https://www.redeszone.net/noticias/seguridad/chatgpt-datos-robados-dark-web/>
2. La Policía Nacional advierte del auge de ciberestafas relacionadas con la Declaración de la Renta. Así puedes protegerte [La Policía Nacional advierte del auge de ciberestafas relacionadas con la Declaración de la Renta. Así puedes protegerte \(genbeta.com\)](#)
3. Avisos del INCIBE de vulnerabilidades en productos comerciales:
 - DELL: Vulnerabilidad crítica - <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-dell>
 - MITSUBISHI: Vulnerabilidad crítica - <https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-mitsubishi-2>
 - ROUTER MOVISTAR 4G: Vulnerabilidad alta - <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-router-movistar-4g>
 - BOSCH: Vulnerabilidad alta - <https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-bosch>
4. También es importante recordar que la última actualización de Microsoft respondía a una serie de vulnerabilidades (algunas críticas y otras consideradas importantes), por lo que es crucial que se actualicen los equipos, incluyendo además smartphones que utilicen Outlook para Android. <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizaciones-de-seguridad-de-microsoft-de-marzo-de-2024>
5. Compartimos un seminario web gratuito que se ha facilitado desde el INCIBE como prevención ante el phishing. De menos de media hora de duración, puede servir para sensibilizar y concienciar sobre esta cuestión: <https://www.incibe.es/incibe-cert/seminarios-web/introduccion-e-identificacion-phishing>
6. Los atacantes que hackearon el Consorcio Regional de Transportes se llevaron los datos personales de 5,5 millones de usuarios madrileños. Ya se ha puesto a la venta en la dark web esta base de datos con nombre y apellidos, nif y dirección completa por un importe de 10K\$. Blog elhacker.NET: Los atacantes que hackearon el Consorcio Regional de Transportes se llevaron los datos personales de 5,5 millones de usuarios madrileños.

Por otra parte, se traslada aviso de **posibles ataques a través de impresoras, cámaras, etc:**

"Una empresa experimentó un ataque de ciberseguridad inusual cuando recibió amenazas a través de su propia impresora, la cual comenzó a imprimir mensajes amenazantes. Este incidente fue el resultado de un ataque de intrusión, destacando la importancia de asegurar todos los dispositivos conectados a la red, incluso aquellos que pueden parecer inofensivos, como las impresoras.

Es un recordatorio vital para las empresas de cualquier tamaño sobre la necesidad de implementar medidas de seguridad cibernética adecuadas para proteger sus sistemas y dispositivos conectados (INCIBE)
."

[Una empresa recibe amenazas a través de su impresora por un ataque de intrusión | INCIBE | INCIBE](#)

¿Qué ha ocurrido? Nos llamó al teléfono 017 del servicio Tu Ayuda de Ciberseguridad un usuario desde una empresa de informática para consultarnos acerca de una de sus impresoras, que tiene conectada en la red, donde había impreso un papel indicando que habían sido hackeados.

www.incibe.es

Para más información, visite <https://binauramonlex.com/contacto/>"