USTIC-AV 08/23. Continúan las campañas de phishing que pretenden conseguir tus datos de acceso

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones **avisa de** que se están detectando en los últimos días **múltiples campañas de correos maliciosos, tipo phishing**, **cuya finalidad es obtener las credenciales de acceso (usuario y contraseña)** a los sistemas informáticos de la Junta de Andalucía.

A los ataques sufridos a finales de la semana pasada, se están sucediendo en las últimas horas otros nuevos que no parece que vayan a ser los últimos, ya que son solo el comienzo de lo que puede acabar siendo un ataque de *ramson ware* como el que están sufriendo otras AA.PP. en general y, servicios sanitarios, en particular.

En esta ocasión, se trata de dos tipos de correos masivos a los empleados de Junta de Andalucía con el aspecto que puedes ver en las imágenes siguientes:

Primer correo fraudulento:

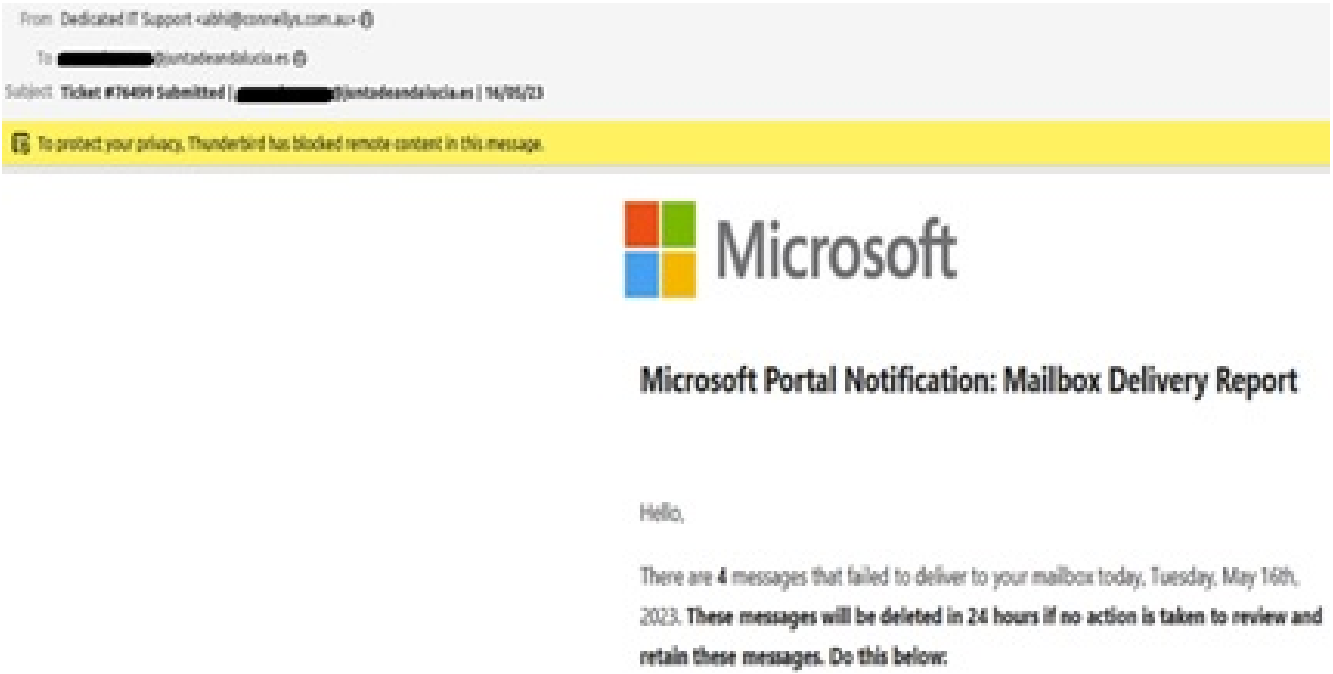


Imagen 1. Correo electrónico malicioso recibido

Si haces clic en el enlace del correo te llevará a esta otra página web, donde te piden tu usuario y clave:

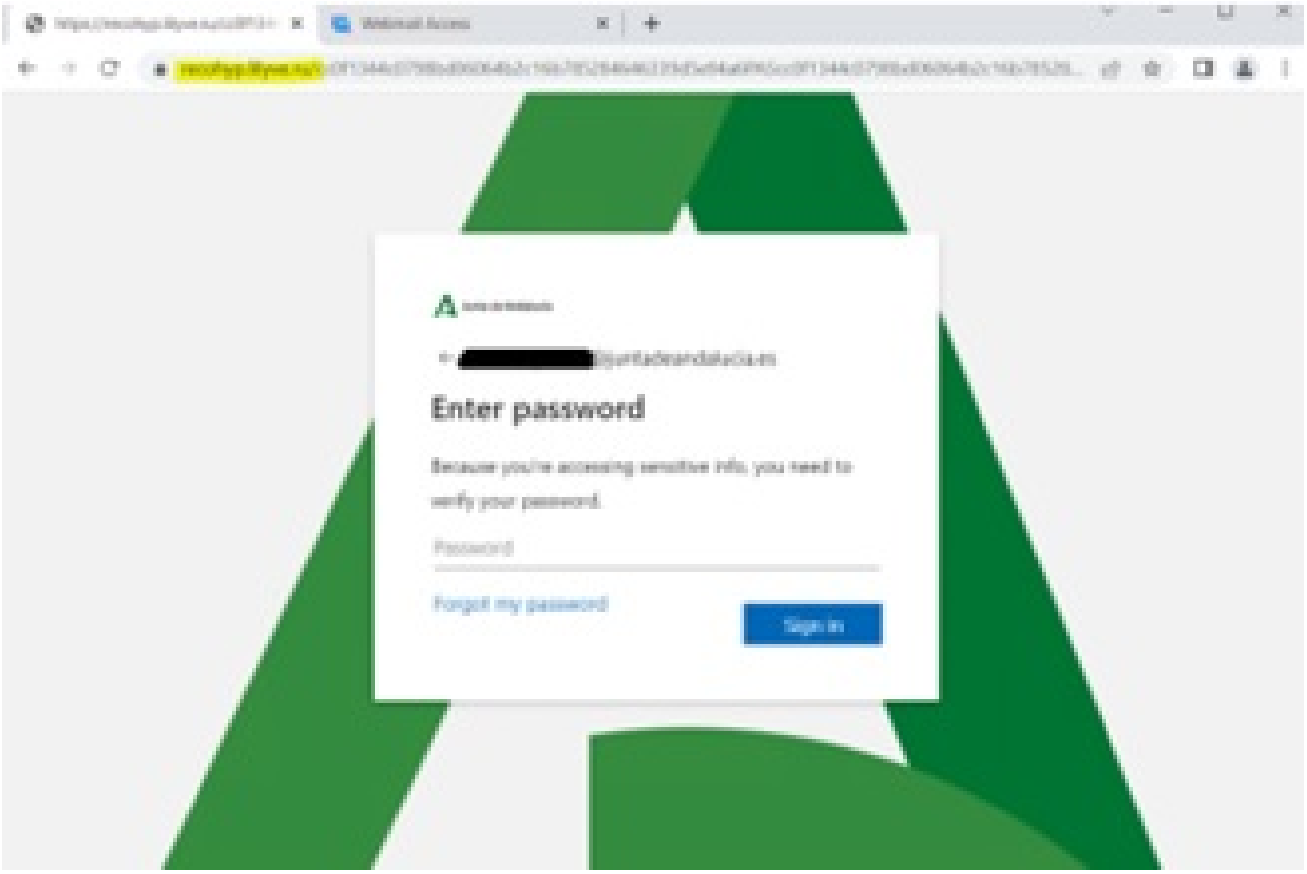
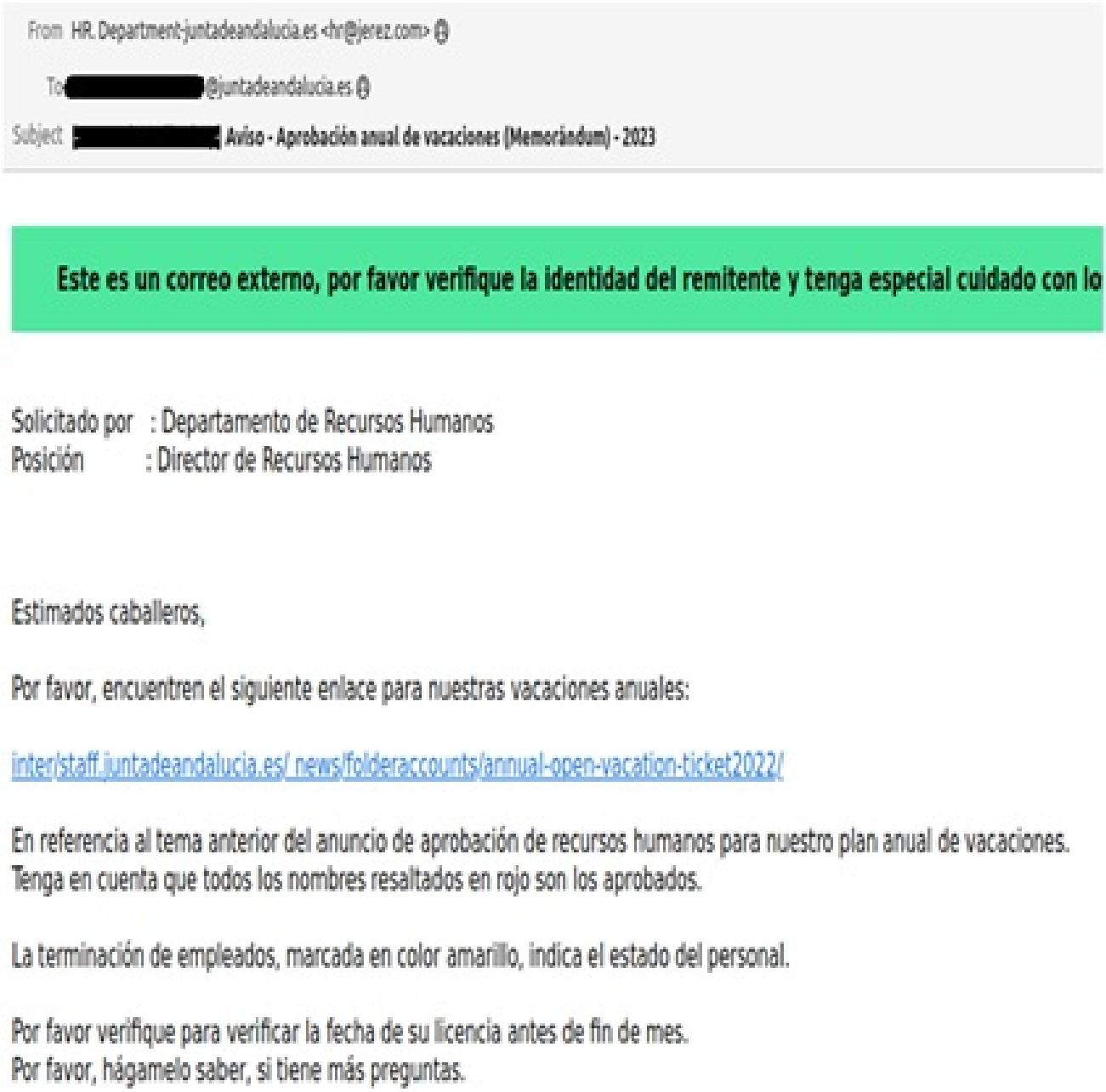


Imagen 2. Falsa página web de la Junta de Andalucía a la que te conduce el mensaje

¡NO PIQUES! Se trata de una página falsa cuyo objetivo es comprometer tus credenciales para luego usarlas en un ataque.

<u>El segundo correo</u> tiene el aspecto siguiente y tiene el mismo objetivo:



From HR. Department-juntadeandalucia.es <hr@jerez.com>

To [redacted]@juntadeandalucia.es

Subject: [redacted] Aviso - Aprobación anual de vacaciones (Memorándum) - 2023

Este es un correo externo, por favor verifique la identidad del remitente y tenga especial cuidado con lo

Solicitado por : Departamento de Recursos Humanos
Posición : Director de Recursos Humanos

Estimados caballeros,

Por favor, encuentren el siguiente enlace para nuestras vacaciones anuales:

inter/staff.juntadeandalucia.es/_news/folderaccounts/annual-open-vacation-ticket2022/

En referencia al tema anterior del anuncio de aprobación de recursos humanos para nuestro plan anual de vacaciones.
Tenga en cuenta que todos los nombres resaltados en rojo son los aprobados.

La terminación de empleados, marcada en color amarillo, indica el estado del personal.

Por favor verifique para verificar la fecha de su licencia antes de fin de mes.
Por favor, hágamelo saber, si tiene más preguntas.

Imagen 3. Segundo correo electrónico malicioso recibido

Si pulsas el link, te lleva a esta otra página web fraudulenta:

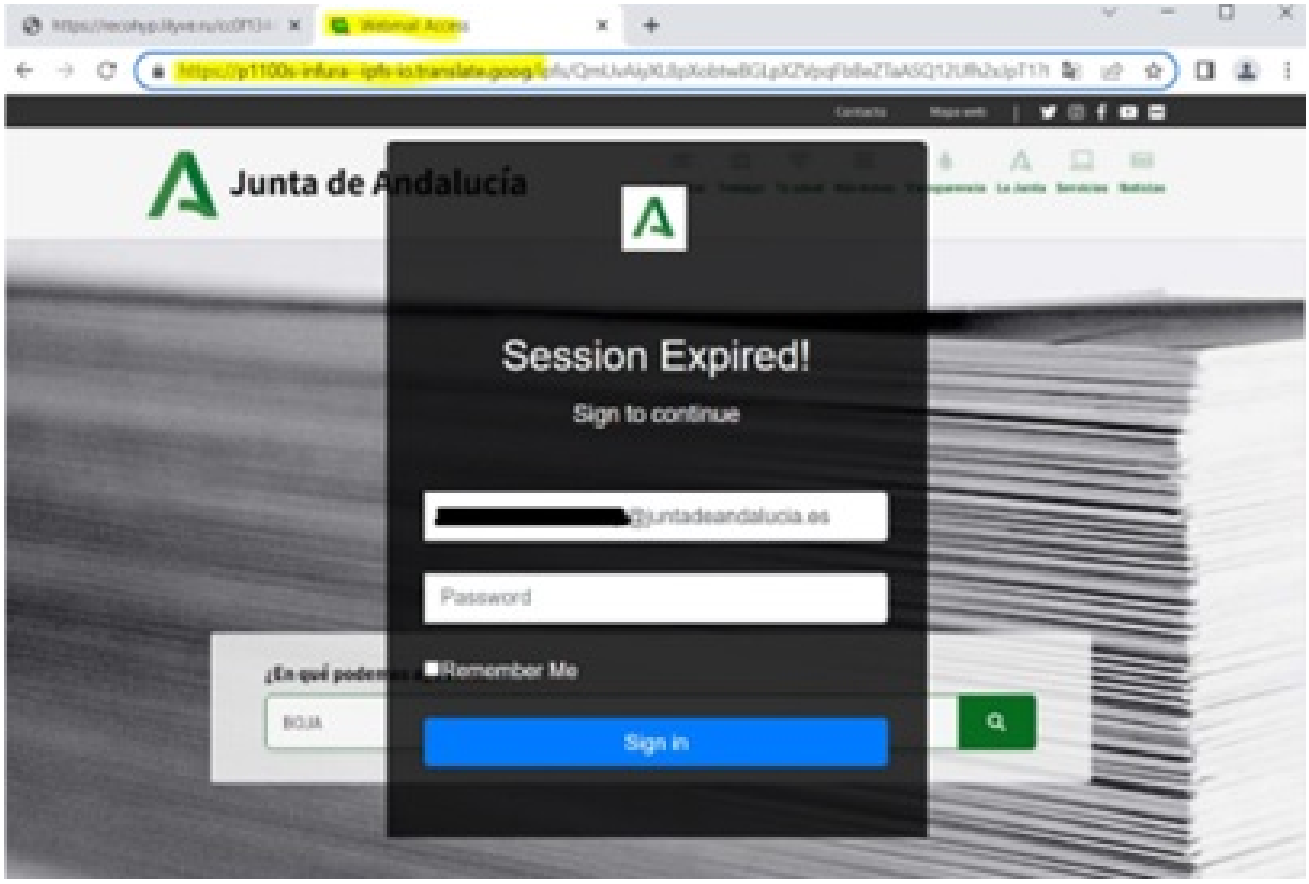


Imagen 4. Falsa página web de la Junta de Andalucía a la que te conduce el mensaje

Al igual que en el anterior caso, **¡NO INTRODUZCAS TUS DATOS!**

Al igual que en los anteriores avisos, os recordamos los pasos que debes seguir:

¿Qué debo hacer si he recibido alguno de ellos?

- **No respondas a estos correo ni pulses los enlaces:**

Podrías comprometer tu información y podría dar lugar a que los ciberdelincuentes realizaran ataques contra los sistemas informáticos de la organización, con el enorme riesgo que eso supondría.

¿Y si he pulsado algún link y he seguido las instrucciones?

Como puedes comprobar, el mensaje enviado simula muy bien las páginas corporativas de la Junta de Andalucía, por lo que es sencillo que hayas podido caer en la trampa. Si es así:

- **Cambia inmediatamente tus claves en AGESCON:** Gestión de cambio de contraseñas (juntadeandalucia.es)

- **Comunica** por cualquier canal de **ayudaDIGITAL esta incidencia**: Contáctanos | ayudaDIGITAL (juntadeandalucia.es)

Recomendaciones

Recientemente os avisamos de otro ataque masivo de correos maliciosos similares solicitando nuestros datos de acceso, por lo que es muy importante que, además de no responder nunca a este tipo de mensajes sospechosos, sigas las siguientes **recomendaciones**:

- *Desconfiar de todos los correos y realizar las comprobaciones oportunas antes de abrir enlaces.*
- *No descargar ningún documento sin estar totalmente seguro del emisor de éste.*
- *No responder a correos electrónico no deseados (SPAM). Se deben mover a la lista de correos no deseados y eliminarlos. Además, configura tu cliente de correos electrónico para filtrar este tipo de mensajes maliciosos.*
- *Evitar la opción de recordar contraseña en los accesos al correo vía web. Además, no compartir credenciales ni información sensible por correo electrónico.*
- *Cuidado con las listas de difusión. Cuando sea necesario enviar un correo con múltiples destinatarios, utilizar la opción de copia oculta.*
- *Comprobar el lenguaje utilizado en el mensaje: Hay que asegurarse de que el cuerpo del correo electrónico no contenga vocabulario poco corriente ni faltas de ortografía. Son indicios de correos maliciosos.*
- *Recuerde que jamás y en ninguna circunstancia debe compartir su contraseña con nadie, así como utilizar sus credenciales de usuario para cuestiones no relacionadas con su trabajo, por ejemplo, páginas o servicios no corporativos.*

Por último, es importante **reportar siempre estos mensajes**, ya que puede haberle llegado a otra persona que no se haya dado cuenta y se pueden aplicar medidas de seguridad para evitar que ese otro usuario caiga. ***¿Cómo se reporta?***

- A la dirección abuse@juntadeandalucia.es
- Siempre que sea posible, hay que mandar el mail sospechoso como adjunto. Para ello, existe la opción de “reenviar como adjunto” en los diferentes clientes de correo como Outlook, Thunderbird o incluso webmail.
- Si no es posible, se puede "reenviar" de manera normal, pero se perderá información valiosa para analizar su procedencia y poder tomar medidas de protección.
- También es posible reportar estos mensajes informando en el área personal de ayudaDIGITAL: https://www.sspa.juntadeandalucia.es/servicioandaluzdesalud/mics/element/r/3850947F36FA01F9A57A001DD8DB1DAE

¡EXTREMA LA PRECAUCIÓN! TEN CUIDADO, NO PIQUES Y DIFUNDE ESTE MENSAJE ENTRE EL RESTO DE PROFESIONALES