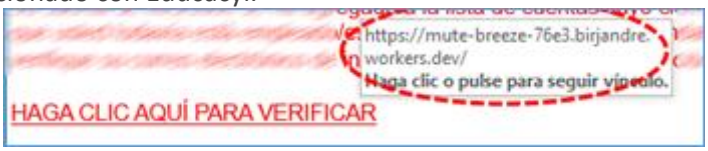
CORREOS FRAUDULENTOS

Buenos días.

Ante las recientes campañas de envío de correos fraudulentos (phishing) creemos conveniente informaros de las siguientes cuestiones:

1. Sobre el ***phishing***:
    - Persigue el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (*suplantación de identidad* de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer *click* en un enlace)
    - Los ***emisores (o remitentes)*** de estos correos normalmente no son conscientes de que se está usando su cuenta de correo para el envío masivo de correos, ya que se produce vía suplantación de identidad al haber estado su contraseña expuesta, o bien, dejando abiertas sus sesiones.

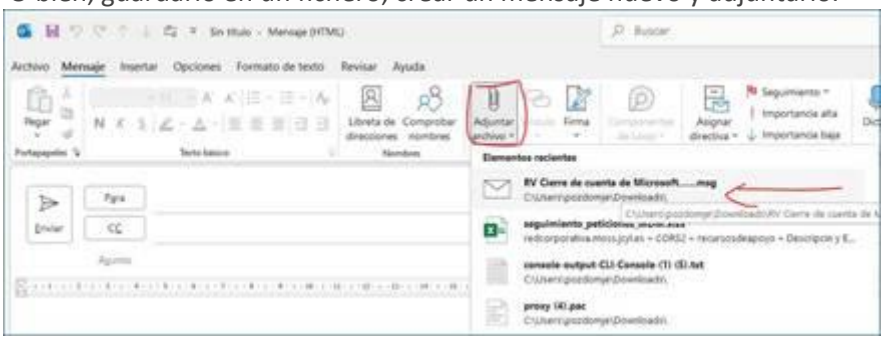
2. **¿Cómo sé si el correo es *sospechoso*?**
    - *Un correo es "sospechoso" si no conoce al remitente o si lo que dice no tiene sentido para usted. Por ejemplo, si le solicitan dinero a ingresar de forma sorpresiva y urgente en una cuenta.*
    - *Los correos pueden leerse, pero* ***nunca pulse en ningún enlace, ni abra ningún adjunto*** *que contengan*.
    - Si tiene dudas de si el enlace es lícito, basta con que sitúe el ratón encima para que se muestre la dirección web real a la que apunta. En el ejemplo, no se indica nada relacionado con Educacyl.



3. **¿Qué se debe hacer** si se recibe un correo sospechoso?
    i. Informarnos reenviando el correo original **como adjunto** a soporte@educa.jcyl.es. *Por favor,* ***no reenvíe*** *el correo como imagen o como un reenvío normal.*

    Para **adjuntar el correo original**, os indicamos 2 posibles formas:
    a. Abrirlo desde Outlook (doble click) y pulsar en reenviar como datos adjuntos.

b. O bien, guardarlo en un fichero, crear un mensaje nuevo y adjuntarlo.



ii. Si por error pulsó en alguno de los enlaces: (que no sean de "*enviar correo a*")

- **Cierre** cualquier página web o aplicación desconocida que se le haya abierto
- **Cierre todas sus sesiones de Microsoft 365** que tenga abiertas.
- **Cambie su contraseña inmediatamente**.

iii. Si no conoce al remitente, marque el correo como *no* deseado (o *spam*)

iv. Elimine el correo.

4. **Acciones con los remitentes**: a los remitentes confirmados de correos *phishing* se les cambia la contraseña de la cuenta Educacyl y se les bloquea el acceso a las aplicaciones Microsoft365. Si estas personas son alumnos, docentes o personal laboral, se informa al centro para que contacte con los afectados.

Como **conclusiones** cabe indicar:

i. La importancia de ***estar concienciados*** de esta realidad y estar alerta. El *phishing* se aprovecha de nuestra dejadez y falta de atención.

ii. Actuar con ***rapidez***, ante la recepción de uno de estos correos, para frenar una posible espiral.

iii. La enorme importancia del ***doble factor de autenticación (2FA)*** ya que, aunque se secuestre la cuenta de alguien, su uso sin permiso es mucho más difícil con este doble factor.