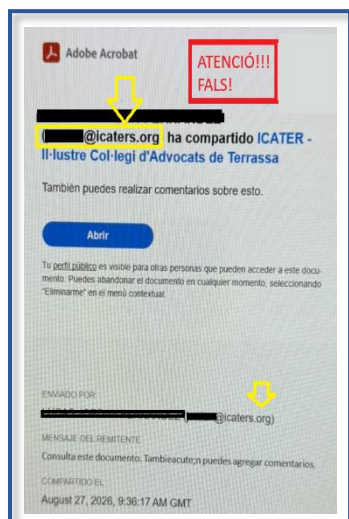




Serveis col·legials



Comunicació núm. 39/2026 – 31 d'agost de 2026

ATENCIÓ! Avís d'intent de phishing a comptes del correu @icater.org – Utilitzen de remitent una adreça SIMILAR a la del nostre domini – però ULL, el domini és fals, és @icaters.

Us trasladem l'avís que ens han fet arribar sobre un intent de phishing que us pot arribar al correu professional fent veure que és un arxiu que us comparteix algun company/a del Col·legi (com veureu a la imatge, el domini del remitent és @icaters.org i el nostre domini REAL és @icater.org, sense la S final).

Os informamos que se ha detectado envíos de correos falsos "phishing" que indican que un compañero/a ha compartido un archivo contigo.

Estos correos incluyen un enlace a un documento en formato pdf o ppt y si os fijáis, el email del remitente, no tiene nada que ver con la dirección real del compañero/a).

Aunque el servicio de Correo incorpora un buen sistema antiSPAM, hay algunos tipos de correo que son difíciles de detectar.

Adicionalmente, y como ayuda general, adjuntamos este enlace de Microsoft con indicaciones de cómo detectar si un correo es fraudulento:

<https://support.microsoft.com/es-es/help/4033787/windows-protect-yourself-from-phishing>

De forma general, recordamos estas recomendaciones de seguridad:

- No abrir correos de usuarios desconocidos.
- No pinchar en enlaces ni abrir adjuntos de mensajes de correo que puedan resultar sospechosos (aunque parezcan venir de usuarios conocidos).
- Utilizar contraseñas robustas y no compartirlas.
- Realizar copias de seguridad con frecuencia.
- Utilizar sistemas antivirus.

