

CONSEJOS Y RECOMENDACIONES SOBRE SEGURIDAD Y PRIVACIDAD EN DOCENCIA ONLINE

1. No abra ningún enlace ni descargue ningún fichero adjunto procedente de un correo electrónico que presente cualquier síntoma o patrón fuera de lo considerado normal o habitual.
2. No confíe únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual, contacte con el mismo por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.
3. Antes de abrir cualquier fichero descargado desde el correo, asegúrese de la extensión y no se fíe por el icono asociado al mismo.
4. No habilite las macros de los documentos ofimáticos incluso si el propio fichero así lo solicita.
5. No debe hacerse clic en ningún enlace que solicite datos personales ni bancarios.
6. Tenga siempre actualizado el sistema operativo, las aplicaciones ofimáticas y el navegador (incluyendo los plugins/extensiones instalados).
7. Utilice herramientas de seguridad, como cortafuegos, para mitigar exploits de manera complementaria al software antivirus.
8. Evite hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.
9. Utilice contraseñas robustas para el acceso al correo electrónico. Las contraseñas deberán ser periódicamente renovadas. Si es posible utilice doble autenticación.
10. Cifre los mensajes de correo que contengan información sensible.

Vicerrectorado de Tecnología y Sostenibilidad
Universidad Complutense de Madrid