EL CORREO ELECTRÓNICO

Riesgos derivados del mal uso

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

metared

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
www.incibe.es

RIESGOS DERIVADOS DEL MAL USO DEL CORREO ELECTRÓNICO

Los ciberdelincuentes no son los únicos que pueden poner en riesgo la seguridad de la universidad, algunas acciones de los usuarios universitarios también pueden ser el origen. La mayoría de los incidentes de seguridad que tienen que ver exclusivamente con el usuario se deben a errores involuntarios. A continuación, detallamos los más frecuentes.

CC y CCO

Enviar correos electrónicos a **múltiples destinatarios usando la opción de CC (Carbon Copy) o en copia, en vez de la opción de CCO o copia oculta (o BCC, Blind Carbon Copy, en algunos casos) es uno de los incidentes de fuga de información** (en este caso, las direcciones de correo de los destinatarios) más comunes en una organización. Cuando se realiza el envío de un correo a múltiples destinatarios, siempre hay que utilizar la opción de CCO de forma que el receptor del correo no vea las direcciones del resto de destinatarios, ya que el correo electrónico es considerado un dato personal y estaríamos divulgándolo sin consentimiento del propietario.

Función de autocompletado

La función de autocompletado puede jugar malas pasadas. En ocasiones cuando se pretende enviar un correo electrónico a un usuario que habitualmente no se utiliza, puede suceder que la función de autocompletado ponga un correo similar gracias a esta función y no nos demos cuenta. Es recomendable deshabilitar esta función siempre que se pueda y en caso de no tener alternativa, **revisar bien el destinatario antes de enviar.**

Descarga automática de imágenes

Tener habilitado en el cliente de correo la descarga automática de imágenes es un riesgo para tu privacidad y seguridad. Las imágenes son usadas para monitorizar si un correo ha sido abierto o no, reduciendo así la privacidad en el uso de esta herramienta de trabajo. Además, dándose las circunstancias adecuadas, la carga automática de imágenes puede ser la puerta de entrada de malware. Siempre es recomendable desactivar esta opción cuando sea posible.