



Uso del correo electrónico... ¡verificar antes de confiar!

“Casi todo delito cibernético se basa en el correo electrónico o lo emplea como parte del proceso”

i

Durante 2019, el 88% de las organizaciones de todo el mundo reconocieron ser víctimas de ataques de suplantación de identidad (phishing), y el 86% que se enfrentaron a ataques con compromiso de cuentas de correo electrónico corporativo

i

Durante la pandemia de COVID-19, en solo un mes se registró un aumento del 667% en estafas de suplantación de identidad (phishing)

i

El 42,8% de todos los adjuntos dañinos fueron documentos de Microsoft Office, o un enlace a dichos documentos

i

Más de 26.000 millones de dólares de pérdidas en 2019 como consecuencia de ataques de compromiso de cuentas de correo electrónico corporativo

i

El 30% de los mensajes de suplantación de identidad (phishing) se entregaron los lunes



Uso del correo electrónico... ¡verificar antes de confiar!

No se registre en sitios de compras con la cuenta corporativa

No haga clic en ningún enlace que solicite datos personales ni bancarios (desconfíe de cualquier solicitud de credenciales o datos personales por medio del correo electrónico)

Si se va a enviar un mensaje a varias personas y se quiere evitar que los destinatarios puedan ver el resto de direcciones, utilice la función de copia oculta (CCO)

Antes de abrir cualquier fichero descargado desde el correo asegúrese de la extensión y no se fíe del icono asociado al mismo

Evite hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido, antes de acceder debe buscar información acerca del mismo en buscadores

Informe inmediatamente al responsable de seguridad seguridad.tic@educacion.gob.es en caso de recibir un correo sospechoso (las faltas de ortografía suelen ser una señal bastante reveladora)

El buzón de la cuenta corporativa de correo tiene una capacidad limitada y no debe utilizarse como repositorio documental

Las herramientas de seguridad Ministerio podrán, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos cuando se detecte un riesgo

Evite utilizar el buzón corporativo para el reenvío automático de correo a buzones ajenos al Ministerio.