Protege tu
información,
protege tu
IDENTIDAD.

# PHISHING

tecnologia@cuc.edu.co

CUC

**EL PHISHING ES UN INTENTO DE SUPLANTACIÓN DE IDENTIDAD DONDE DELINCUENTES BUSCAN ENGAÑARTE PARA ROBAR INFORMACIÓN PERSONAL, FINANCIERA O INSTITUCIONAL.**

# Señales de alerta en un correo sospechoso

El remitente parece extraño o no coincide con la entidad oficial.

Mensajes con tono urgente o alarmante: "actúa ahora", "última oportunidad", "evita sanciones".

Solicitan información personal, contraseñas o diligenciar formularios.

Contienen errores de ortografía, redacción o logos mal editados.

Incluyen enlaces o archivos adjuntos poco confiables.

## ¿Recibiste un correo sospechoso?

No respondas, y repórtalo de inmediato como sospechoso al Departamento de Tecnología

tecnologia@cuc.edu.co

CUC

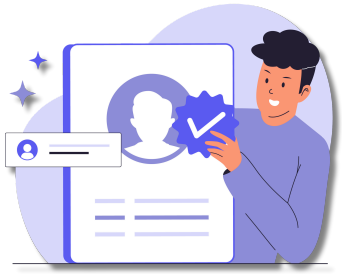
# RECOMENDACIONES

## ¡Nunca solicitaremos tu contraseña por correo electrónico o por teléfono!

Por tu seguridad, cambia tu contraseña cada 6 meses, tal como indica nuestra política institucional.

Activa la MFA (doble autenticación) para mayor seguridad.

Verifica siempre el remitente y el contenido. Las instituciones más suplantadas son bancos, DIAN, Registraduría Nacional y campañas de vacunación.



### ¿Recibiste un correo sospechoso?

No respondas, y repórtalo de inmediato como sospechoso al Departamento de Tecnología

tecnologia@cuc.edu.co

CUC