¿Qué es un correo fraudulento?

El correo electrónico fraudulento es el que proviene de un remitente falso o que no pertenece al servicio legítimo de Correos que aparenta. Usualmente viene con "***Asuntos***" llamativos, impactantes o alarmantes para ejercer presión, curiosidad o temor a los usuarios que los reciben.

¿Cómo identificamos un correo fraudulento?

Éstos correos fraudulentos normalmente contienen link o enlaces sospechosos o archivos adjuntos que le invitan a dar clic o abrirlos.

- La Unidad de Informática y Sistemas jamás les solicitará que confirmen sus cuentas o contraseñas o que se registren en algún sitio con credenciales de correo.
- Usualmente los mensajes vienen con direcciones de correo que no provienen de dominios conocidos o seguros, nuestro dominio es **cultura.gob.sv.** Un ejemplo de correo con dominio inseguro es: phenduike@**durbs.com**

Manejo de correos electrónicos fraudulentos

- **No hagas clic** en ningún enlace que contenga.
- **No respondas al correo electrónico o mensaje recibido**. Si tienes dudas, puedes reportarlo a esta unidad.
- **Elimina** este tipo de correos de bandejas de Entrada y Papelera.

Consejos para evitar recibir correos maliciosos

1. No hagas clic en link o enlaces que no sean seguros.
2. No publiques tu cuenta de correo en ningún web.
3. No te registres en páginas web que no inspiren confianza.
4. Elimina directamente los correos fraudulentos que recibes, sin abrirlos ni contestarlos.

NOTA:

Pese a la seguridad en plataforma de correo o antivirus en los equipos, siempre se cuelan correos fraudulentos, que buscan obtener repuesta del usuario para capturar contraseñas, infiltrar virus o comprobar que detrás de la cuenta hay una persona física. Por ello, es importante eliminar estos correos directamente, sin abrirlos ni contestarlos para evitar que archivos maliciosos se filtren a nuestros equipos.