

LA IMPORTANCIA DE NO INGRESAR TUS CREDENCIALES

EN SITIOS FALSOS

Una "credencial" se compone de un **usuario y contraseña**; son los **datos de acceso** a plataformas y/o aplicaciones.



Los ciberatacantes lanzan campañas de phishing con el objetivo de confundirte. El cuerpo del mensaje suele variar pero la estructura y objetivo son los mismos:

¡Robar tus accesos!

¡SOSPECHA!

Si el correo te indica **que la contraseña va a caducar pronto, hay una nueva actualización del servicio** y no se puede seguir utilizando a partir de XX fecha.

Asegúrate de que el destinatario es legítimo.

ACTUALIZA AQUÍ

<https://websmail.contrOI536HDgtñil>

¡DESCONFÍA!

Si en el texto del correo el destinatario **te incita a dar click en un enlace fraudulento** para cambiar tu contraseña o actualizarla.

Nunca des click sin antes pasar el cursor encima del link o botón y verificar que es real.

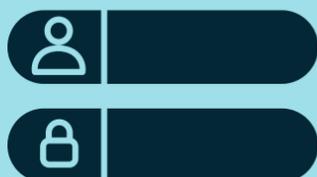
¡NO LO CREAS!

Si en el texto del correo **te solicitan directamente los datos de acceso**; informándote que ejecutarán los cambios de manera automática.

Nunca entregues tus datos personales.



¿CAÍSTE?



¡ACTUALIZALAS Y ACTIVA EL MFA!

¡No lo ocultes o minimices, es muy importante que lo notifiques!

Repórtalo inmediatamente con el área de seguridad.

TU LOGO AQUÍ

