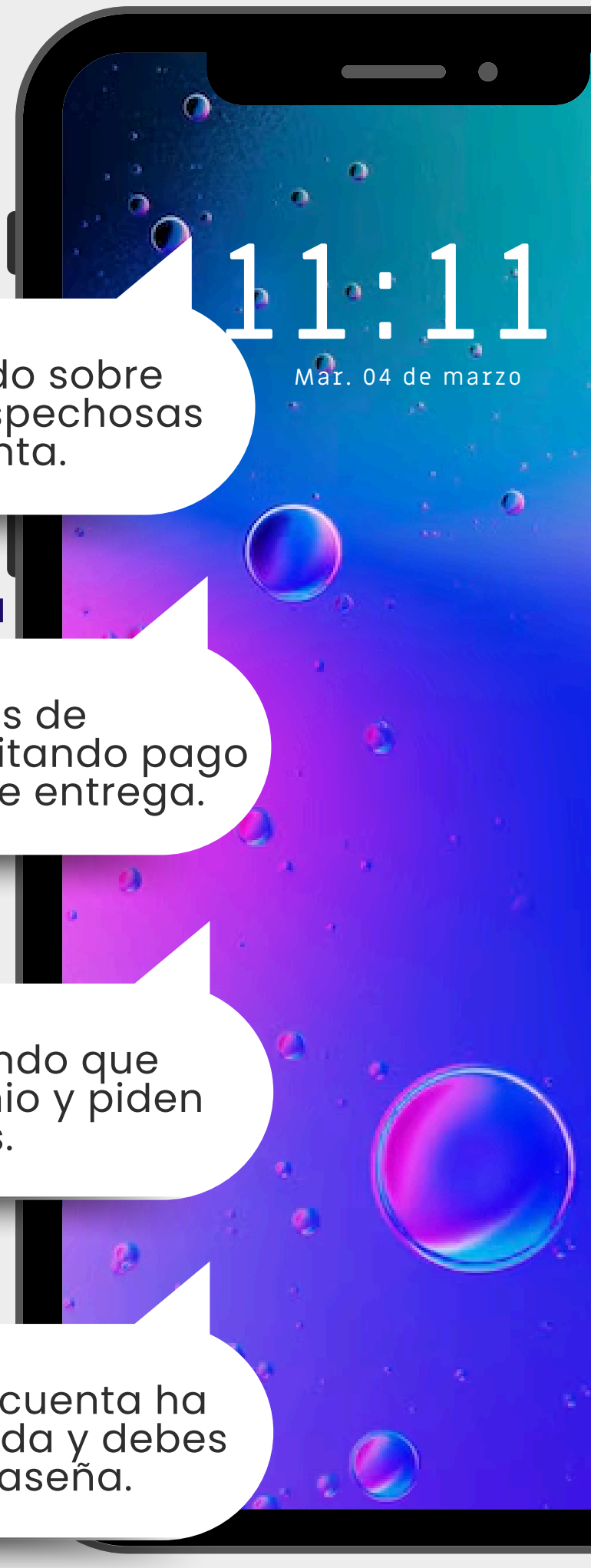
CASOS COMUNES DE SMISHING

Y CÓMO EVITARLOS.

El smishing es un fraude por SMS donde los atacantes suplantan entidades confiables para robar datos o infectar dispositivos mediante enlaces maliciosos.



Avisos bancarios

Mensajes alertando sobre transacciones sospechosas o bloqueo de cuenta.

Paquetes de entrega

SMS de "empresas de mensajería" solicitando pago o confirmación de entrega.

Premios y sorteos

Mensajes afirmando que ganaste un premio y piden datos personales.

Soporte técnico

Avisos de que tu cuenta ha sido comprometida y debes cambiar tu contraseña.

¿CÓMO EVITAR CAER EN SMISHING?

- ✅ No hagas clic en enlaces sospechosos
- ✅ Verifica directamente con la empresa o persona
- ✅ No compartas información personal por SMS
- ✅ Habilita la autenticación en dos pasos (2FA)

SI RECIBES UN SMS QUE TE PAREZCA SOSPECHOSO, CONFÍA EN TU INSTINTO Y REPÓRTALO.

TU LOGO AQUÍ

Grupo Smartekh | Security Culture Management