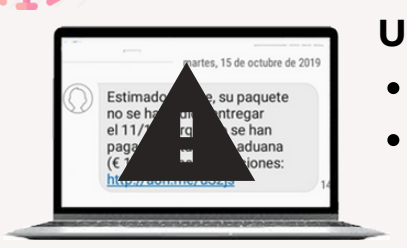
5 SEÑALES PARA IDENTIFICAR SI UN CORREO SOBRE EL COVID-19 ES PHISHING

"Protege aquello que te mantiene conectado"

1 Recurre al miedo o la urgencia



Un E-mail de una fuente legítima NUNCA

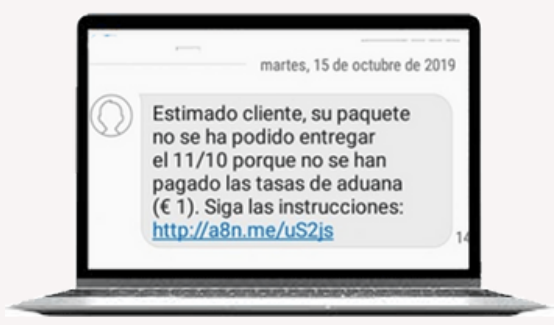
- Utiliza asuntos o vocabulario alarmista que incite al pánico,
- Incluye mensajes que revelen nuevos casos en tu ciudad en forma de link o botón para descarga o redirección.

Si recurre al sentido de urgencia ES PHISHING

2 Te solicita información sensible, como tus contraseñas y datos de tarjetas

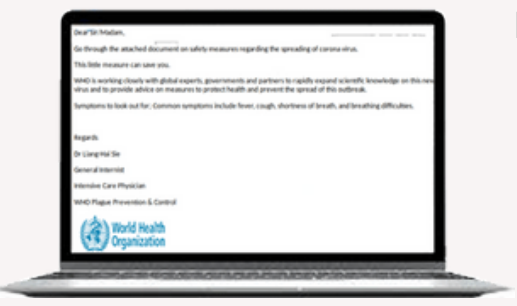
SIEMPRE sospecha de todo correo que . . .

- Te pida información personal y/o sensible.
- Incluya links acortados.
- Solicite credenciales de autenticación e información financiera.



Si te pide información sensible ES PHISHING

3 Usa lenguaje inusual como un saludo poco común



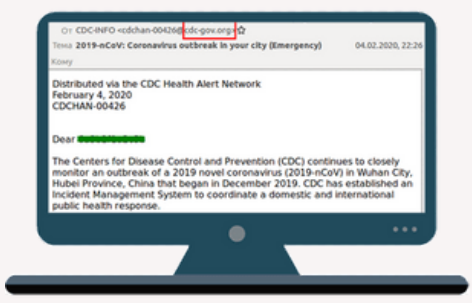
NUNCA confies en un correo que utiliza un lenguaje poco usual. . .

- Un saludo poco común: *"Sir/Madame"*.
- Signos o símbolos *$%&#!* entre líneas.
- Términos muy ambiguos.

Si el lenguaje es muy extraño ES PHISHING

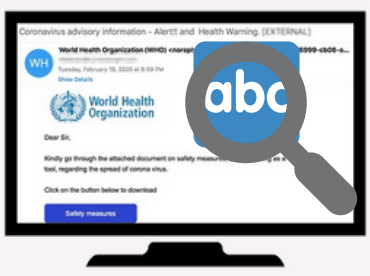
4 Proviene de una dirección de email incompleta y/o desconocida

SIEMPRE sospecha de todo correo que venga de dominios **desconocidos, extraños, incompletos** o bien, que provengan de supuesta organización en la que están combatiendo el **COVID-19.**



Si viene de dominio sospechoso ES PHISHING

5 Contiene errores de ortografía, de sintáxis y gramáticales



La mayoría de las campañas del phishing sobre el **COVID-19** son en inglés. **NUNCA** confies en el correo si incluye muchos errores ortográficos o la redacción no tiene sentido ni coherencia .

Si tiene mala gramática/ortografía ES PHISHING

FUENTES: FORBES 2020. CORONAVIRUS SCAM ALERT. & RISK MANAGEMENT MONITOR 2020 CORONAVIRUS RELATED PHISHING EMAILS

WWW.SMARTEKH.COM