CÓMO IDENTIFICAR ATAQUES DE INGENIERÍA SOCIAL 2



1. Comprobar el remitente (*phishing*, *smishing* y *vishing*): si coincide con la _____ o entidad remitente, podemos estar _____. Sin embargo, si no _____, nos aparece un número _____ o un correo _____, se trata de un _____.

2. **Analizar el asunto (*phishing*)**: la mayoría de _____ utilizarán un asunto _____ que capte nuestra _____ para que ignoremos el resto de _____.

3. Analizar el objetivo del mensaje (*phishing, smishing* y *vishing*): debemos _____ qué quieren de _____. Si es una entidad como nuestro _____, lo más probable es que ya tenga nuestros _____ y no necesite volver a pedírnoslos. Estos _____ suelen solicitar llevar a cabo una acción de manera _____, para evitar que nos paremos a _____ el mensaje, por ello es probable que se trate de un _____.

4. Examinar la redacción (*phishing* y *smishing*): los errores _____ y _____ son _____ de mensajes _____ con _____ o mediante una traducción _____, lo que debe hacernos _____.

incibe_ 017 OSI POLICIA NACIONAL
LIVEWORKSHEETS