## Lista de comprobación para la concienciación sobre el phishing

#### Manténgase alerta y use esta lista de verificación para determinar rápidamente si un mensaje extraño podría ser un ataque de phishing.

#### 4 formas de detectar un phish

1. **Verifique el encabezado**

* ¿Le he dado mi dirección de correo electrónico a esta empresa antes?
* ¿Tengo una cuenta con esta empresa?
* ¿La identidad del remitente coincide con la finalidad del correo electrónico?
* ¿Mi correo electrónico está en la lista de direcciones De:?
* ¿La dirección Para: está dirigida a destinatarios no revelados o a un gran número de destinatarios que no conoce?

1. **Verifique el contenido**

* ¿Los enlaces proporcionados en el cuerpo del correo electrónico parecen válidos?
* ¿Hay errores ortográficos y tipográficos? ¿Cómo es la gramática y el tono apropiado?
* ¿Me están prometiendo mucho dinero a cambio de poco o ningún esfuerzo por mi parte?
* ¿Se me pide que aporte dinero por adelantado para actividades dudosas, una tasa de tramitación o que pague el coste   
  de agilizar el proceso?
* ¿Alguien me pide mi número de cuenta bancaria, otros datos financieros personales o contraseñas?   
  ("Verifique su cuenta" o "Haga clic en el enlace a continuación para obtener acceso a su cuenta" son comunes)

1. **Considere la finalidad del correo electrónico**

* ¿El problema realmente es tan urgente como lo hace ver el remitente?
  + "Si no responde en 48 horas, su cuenta se cerrará".
  + "Si no lo hace, es posible que su cuenta se desactive automáticamente".
* ¿Por qué el remitente solicita confidencialidad? ¿Cómo puedo saber si la actividad propuesta es legítima y auténtica?

1. **Tenga cuidado con los archivos adjuntos**

* No abra archivos adjuntos inesperados.
* No abra archivos adjuntos de extraños. Asegúrese siempre de conocer primero al remitente.
* No abra archivos adjuntos inusuales.
* No abra archivos adjuntos que vengan con mensajes de apariencia extraña.