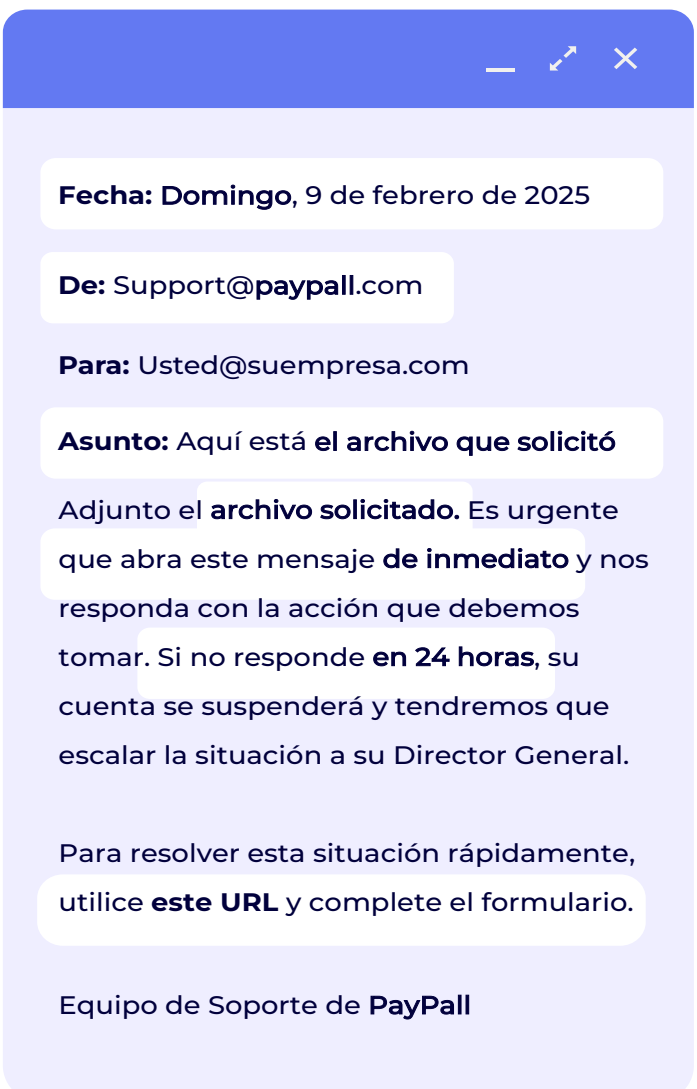
Manténgase protegido. Conozca cómo detectar un correo electrónico falso.

Según un informe de Verizon de 2024, 90 % de las violaciones de seguridad comienzan con un correo electrónico de phishing. Reduzca el riesgo aprendiendo a identificar correos electrónicos potencialmente peligrosos con estos consejos.



- **Revise cuándo fue enviado el correo:** Envíos durante fines de semana o fuera de horarios laborales son señales de alerta.
- **Revise quién envía el correo:** Empresas legítimas tienen correos corporativos. Identifique errores de ortografía o dominios extraños.
- **Contenido genérico o confuso:** Puede incluir saludos genéricos como "Estimado cliente," asuntos que no corresponden al contenido del correo o archivos adjuntos no solicitados.
- **Desconfíe de archivos adjuntos:** Especialmente si no lo estaba esperando, o son tipos de archivos inusuales que podrían contener malware.
- **Lenguaje de urgencia:** Frases como: 'responda inmediatamente,' o 'actúe ya o su cuenta será suspendida' son sospechosos.
- **Errores de gramática:** Con el uso de IA, los correos de phishing son casi perfectos, pero sea precavido y revise bien el contenido.
- **Identifique vínculos falsos antes de hacer clic:** Pase el cursor sobre los enlaces para ver la URL. Si no coincide con el mensaje, no es el sitio web oficial de la empresa o el enlace lleva a un sitio web desconocido, ¡no haga clic!

Haga clic con inteligencia: Proteja a su empresa.

Contáctenos hoy mismo para que le ayudemos a capacitar a su equipo para identificar correos electrónicos de phishing y para asegurar los sistemas de correo electrónico de su organización. Con un aumento del 60 % en el ransomware distribuido por correo electrónico el año pasado (Cybersecurity Ventures, 2024), es más necesario que nunca mantenerse alerta y tomar medidas proactivas para la protección de su empresa. Juntos, podemos reducir el riesgo de las ciberamenazas.

Cubical
Correo: soporte@cubical.ec Teléfono: +59325142100
http://www.cubical.ec