CONCIENTIZACIÓN SOBRE LA SEGURIDAD CIBERNÉTICA

CUIDADO CON LOS ATAQUES DE SPYWARE Y PHISHING

Mantengámonos alerta ante los peligros de los ataques de **phishing** y **spyware**.

¿QUÉ ES SPYWARE?

Las estafas o fraudes de spyware involucran a individuos o grupos que intentan engañarle para que instale un software malicioso en su computador o dispositivo. Una vez instalado, ese software puede permitir a los atacantes robar su información personal, incluyendo contraseñas e información financiera, e incluso tiene la capacidad de controlar su dispositivo de manera remota.

¿QUÉ ES PHISHING?

Las estafas o fraudes de phishing adoptan la forma de correos electrónicos o sitios web falsos que parecen legítimos, pero están diseñados para robar información personal como contraseñas, números de tarjetas de crédito y datos de cuentas bancarias.

SI NOTA ALGO SOSPECHOSO, ¡REPÓRTELO!

Si usted recibió un correo electrónico sospechoso, por favor repórtelo enviando un correo electrónico a: **phishing-dpdhl@dhl.com** y agregue el correo sospechoso como un archivo adjunto. Para enviar un correo electrónico como un archivo adjunto a través de Outlook, diríjase a Insertar > Elemento de Outlook y seleccione el correo electrónico que va a adjuntar.

Para más información, visite nuestra página de Alerta de Fraude en dhl.com.

LAS 4 MEJORES PRÁCTICAS DE LA SEGURIDAD CIBERNÉTICA

1. Sea cuidadoso al abrir correos electrónicos o al hacer clic en enlaces de fuentes desconocidas. Verifique siempre que los correos electrónicos y enlaces que parezcan proceder de DHL sean de sitios web y direcciones de correo electrónico legítimos de DHL, y no falsificaciones. Para esto, revise detenidamente la URL o la dirección de correo electrónico. Si no está seguro, por favor póngase en contacto con nuestro equipo global a través del correo electrónico: **phishing-dpdhl@dhl.com**.

2. No ingrese su información personal en sitios web sospechosos.

3. Mantenga actualizado el software de antivirus en su computador al igual que el resto del software, según las solicitudes de la red para actualizar su sistema, hágalo lo más pronto posible.

4. Desconfíe de las ventanas emergentes o las descargas inesperadas.

PT 08399 041923