DHL

CYBERSECURITY AWARENESS
WATCHING OUT FOR SPYWARE AND PHISHING ATTACKS

Let's stay alert to the dangers of **phishing** and **spyware** attacks.

WHAT IS SPYWARE?

Spyware involves individuals or groups who try to trick you into installing malicious software on your computer or device. Once installed, this software can allow the attackers to steal your personal information, including passwords and financial information, and even has the ability to control your device remotely.

WHAT IS PHISHING?

Phishing scams take the form of fake emails or websites that appear legitimate but are designed to steal personal information such as passwords, credit card numbers, and bank account details.

SPOT SOMETHING SUSPICIOUS? REPORT IT!

If you received a suspicious email, report it to: **phishing-dpdhl@dhl.com** and include the suspected email as an attachment. To send an email as an attachment in Outlook, go to Insert > Outlook Item and click on the email in question.

For more information, see our Fraud Awareness page at dhl.com.

TOP 4 CYBERSECRUITY BEST PRACTICES

1. Be **cautious** when **opening emails** or **clicking on links** from unknown sources. Always **verify** that emails and links that appear to come from DHL are from legitimate DHL websites and email addresses, not fakes, by **closely checking the URL or email address it was sent from**. If you're not sure, contact our global team at **phishing-dpdhl@dhl.com**.

2. **Don't** enter your **personal information** on **suspicious websites**.

3. Keep your computer's antivirus **software** and all other software **up to date** by responding to network requests for updates to your system as soon as possible.

4. Be wary of **pop-up windows** or **unexpected downloads**.