

Holiday Phishing

Cyber criminals take advantage of the holidays to disguise their phishing campaigns and malware as seasonally accepted email. Requests for donations to fraudulent organizations, bogus holiday advertisements, and posing as package delivery services are common this time of year. Below is a real example of a phishing email impersonating Federal Express.

From: Fedex tracking Express
Appears to come from a trusted sender

Date: November 19, 2018 at 6:23:08 AM CST

To: <alanham@reliantpacs.com>

Subject: Notification: Your parcel status has changed
Actual email address is not recognizable

No address information

We sent your parcel on Reliantpacs to your address on 11/19/2018 04:23:08 am and it returned back today due to invalid address. Your recent address is required to enable us deliver your parcel. ← Bad grammer

- Updated location required.
- Correct mobile number for delivery.
- Kindly visit the below to update your details today.

Link is not recognizable

<="" href="https://www.eeizo.com?u=YWxhbmhhbUByZWxpYW50cGFjcy5jb20=" rel="noopener noreferrer" target="_blank" data-auth="NotApplicable">Update Reliantpacs Address

What to Do If You Suspect You Are Victim of Phishing

- Change your password immediately
- Contact your IT Department. For Reliant employees contact support@reliant-rehab or call 225-767-7670.