

Phishing Alert - Watch For Fraudulent Package Delivery Emails

Scammers take every opportunity to trick you into doing what they want and the holidays are no exception. Here's how their holiday package delivery con typically works: They send you an email (claiming to be from FedEx, UPS, etc.) that describes a missed delivery or shipping address problem and tells you to click on a link to correct the issue. The link goes to a spoofed website which attempts to gather critical information like passwords, Social Security numbers, credit card numbers, and more. Don't be fooled. The FedEx website says, "FedEx does not request, via unsolicited mail or email, payment or personal information in return for goods in transit or in FedEx custody." The same is true for the other major package delivery services.



Another similar trick is an email supposedly from the U.S. Postal Service regarding an intercepted package delivery. The email contains a link that, when activated, installs a virus that steals personal information on your computer. Sometimes these emails elicit a sense of false urgency by stating that if you do nothing, you will be charged money.

The best way to combat this type of scam is to avoid opening suspicious, unsolicited emails or clicking on links within them. Warning signs of bogus emails include:

- Unexpected requests for money
- Requests for personal information
- Links to familiar-looking websites that are actually spelled wrong
- Extensive spelling and grammar errors in the body of the email

You can also adjust the settings in your email application to capture more spam in a junk folder. When you do see emails like these in your inbox, delete them immediately.