

Safe to Open? 5 Signs to Check First

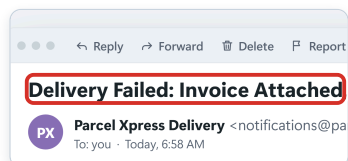
What to look for before you double-click an email attachment, and what to do if you already did.



*We Make
I.T.
Happen!™*

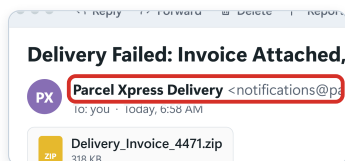
1 Were You Expecting It?

An invoice or delivery notice you **weren't expecting** is the biggest red flag.



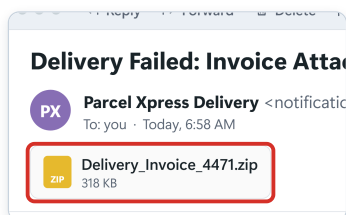
2 Check the Sender

The name looks official, but the **real address** is a strange, unrelated domain.



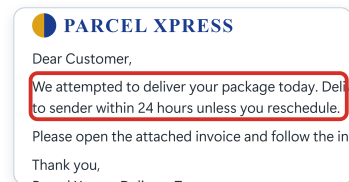
3 The Real File Type

A **ZIP, EXE, SCR, JS or VBS** file is far riskier than a plain PDF or photo.



4 Urgent or Scary Wording

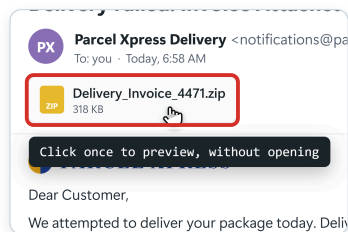
"Returned within 24 hours" is designed to make you **open it before you think**.



Real shipping companies don't threaten you by email.

5 Preview, Don't Open

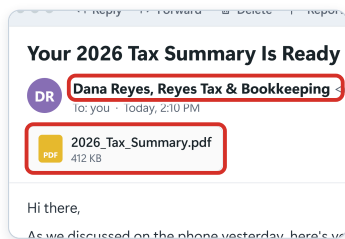
Outlook and Gmail can show an attachment in a **preview pane** first.



Only open it in the full program if it looks right.

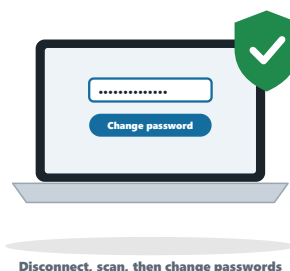
6 Not Every Attachment Is Risky

Expected, from someone you know, in a file type that **matches**: that's normal.



7 Already Opened One?

Disconnect from Wi-Fi, run a **full antivirus scan**, and **change your passwords** from a clean device.



8 Still Not Sure?

When in doubt, **don't open it**. Verify with the sender first.



**Call us before you open it:
239-513-1960**



Good to Know

- A file can be named **invoice.pdf.exe** to hide its real extension. Turn on **File name extensions** in File Explorer's View tab.
- Scammers can **spoof** a real contact's name. An unexpected file from someone you know still deserves a second look.
- Already opened a risky one? Call **239-513-1960** and we'll check your computer.



Need Help?

Contact Naples Computers
239-513-1960
We Make I.T. Happen!™