

NAPLES COMPUTERS HOW-TO • EMAIL SECURITY

How to Safely Open an Email Attachment

Not every email attachment is dangerous, but some absolutely are. Scammers attach fake invoices, delivery notices and other files that quietly install malware or steal passwords the moment you open them. This guide covers five warning signs to check first: whether you were expecting the file, the sender's real address, the real file type, urgent or scary wording, and previewing an attachment instead of opening it, plus what a normal, expected attachment looks like.

Why attachments are risky

A single attachment can quietly install malware, lock your files for ransom, or steal a password, often the moment it opens.

Hidden malware

A single click can quietly install malware or ransomware on your computer.

Fake file types

A file named invoice.pdf.exe isn't really a PDF, it just looks like one.

Stolen logins

A file that asks you to "enable content" or sign in again can steal your password.

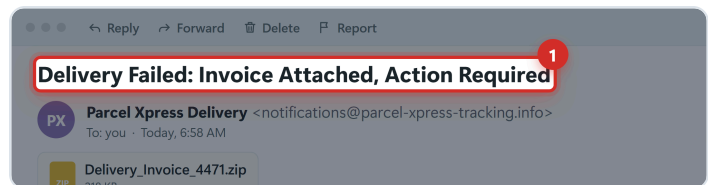
The 5 warning signs

1 Were you expecting it?

An invoice, delivery notice or file you weren't expecting is the biggest red flag of all.

WHAT TO DO

Didn't order anything, or didn't ask for this file? Treat it as suspicious.

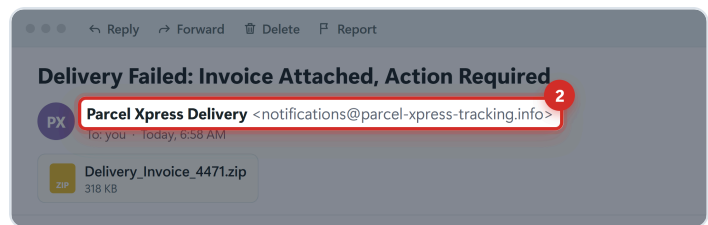


2 Check the sender's address

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

WHAT TO DO

Look at the full email address, not just the display name.

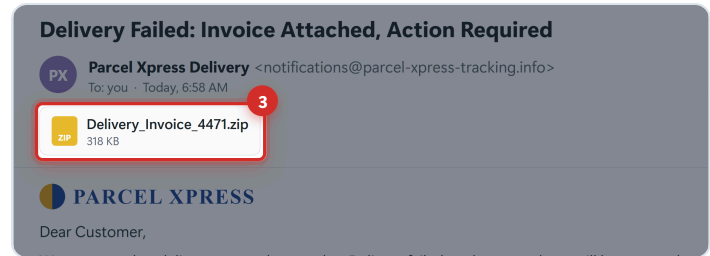


3 Look at the real file type

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

WHAT TO DO

On Windows, turn on "File name extensions" in File Explorer's View tab to see the real extension.

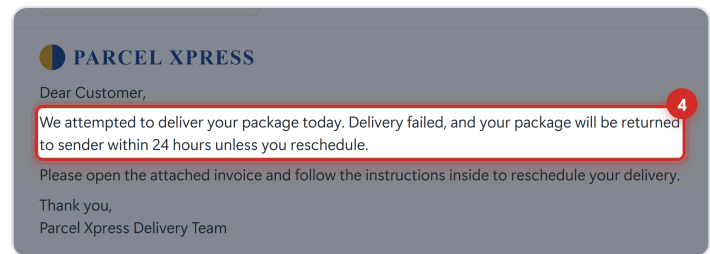


4 Urgent or scary wording

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

WHAT TO DO

Slow down. Real shipping companies don't threaten you by email.

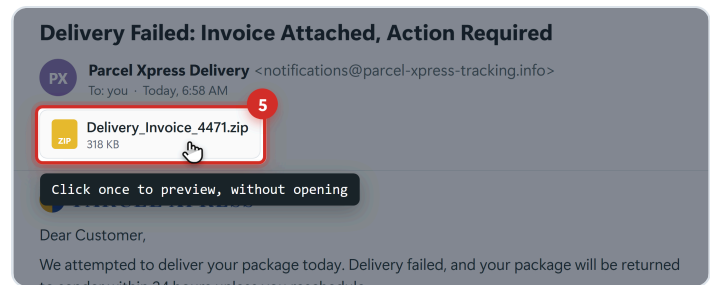


5 Preview it, don't open it

Outlook and Gmail can show you an attachment without fully opening it in its own program.

WHAT TO DO

Click once to preview. Only open it in the full program if it looks right, and you were expecting it.



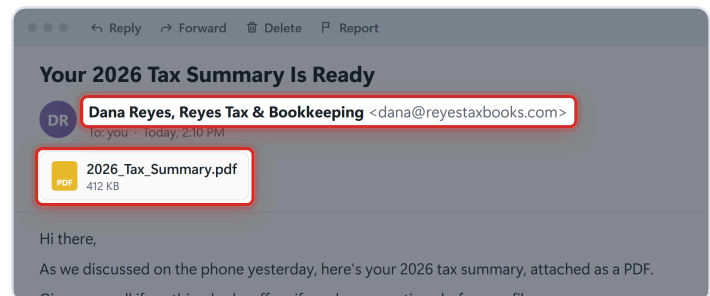
GOOD TO KNOW

! Not every attachment is dangerous

A PDF from someone you already know, that you were expecting, after a call or a conversation, is normal.

WHY THIS ONE'S FINE

You were expecting it, you know the sender, and the file type matches: this one is fine to open.



Already opened one? **Act fast.**

- ☐ Disconnect from Wi-Fi, or unplug the network cable
Stops malware from spreading, or sending out your data
- ☐ Run a full antivirus or anti-malware scan
Microsoft Defender works; let it finish completely before you use the computer again
- ☐ Change your passwords from a different, clean device
Start with email and banking
- ☐ Call Naples Computers: 239-513-1960
The sooner we check it, the better

Recap: **safely open an attachment**

- | | |
|--|--|
| ☐ Were you expecting it? | ☐ Preview it, don't open it |
| ☐ Check the sender's address | ☐ Not every attachment is dangerous |
| ☐ Look at the real file type | ☐ Already opened one? Scan right away |
| ☐ Watch for urgent, scary wording | ☐ Still unsure? Call us first |

When in doubt, don't open it. Save the attachment without opening it, and verify with the sender using a phone number or contact you already have, not a number from the email itself. Already opened a risky one? Disconnect from the internet, run a full antivirus scan, change your passwords from a clean device, and call us at 239-513-1960.



Not sure about an attachment, or think you've already opened a risky one?

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**