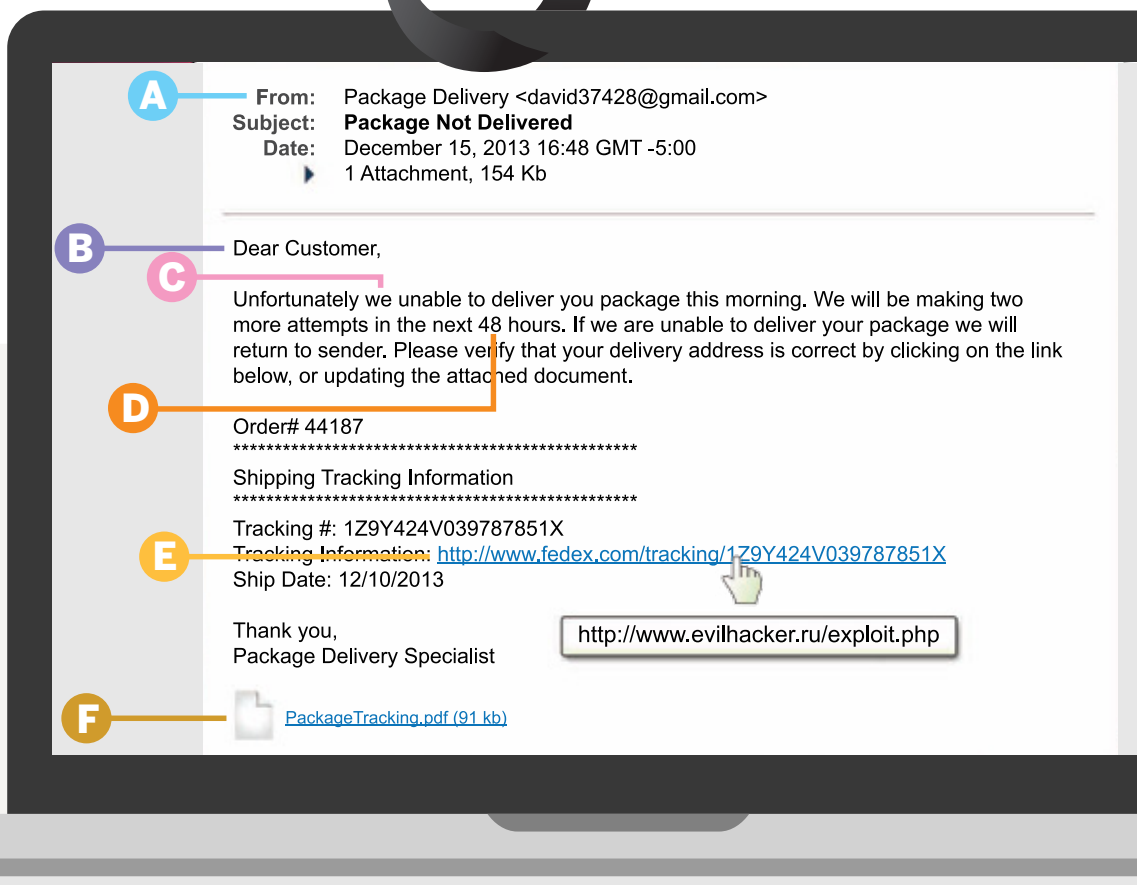
Don't get HOOKED

La Capitale

You have probably already received phishing messages on your work or personal (gmail.com, hotmail.com, etc.) email address. *If you click the links included in these messages or open attachments, you may be in for some nasty surprises.* Don't bite the hook that fraudsters dangle in front of you!



A **CHECK THE EMAIL ADDRESSES.** If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?

B Be suspicious of emails addressed to "Dear Customer" or that use some other **GENERIC SALUTATION.** If a trusted organization has a need to contact you, they should know your name and information. Also ask yourself, am I expecting an email from this company?

C Be suspicious of **GRAMMAR OR SPELLING MISTAKES;** most businesses proofread their messages carefully before sending them.

D Be suspicious of any email that requires **"IMMEDIATE ACTION"** or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.

E **BE CAREFUL WITH LINKS,** and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different than what is shown in the email, this is an indication of an attack.

F **BE SUSPICIOUS OF ATTACHMENTS.** Only click on those you are expecting.

! Be suspicious of any message that **SOUNDS TOO GOOD TO BE TRUE.** (No, you did not just win the lottery.)

!! Just because you got an **EMAIL FROM YOUR FRIEND** does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.

If you believe you have received a fraudulent e-mail, please forward it to **frauds@lacapitale.com**