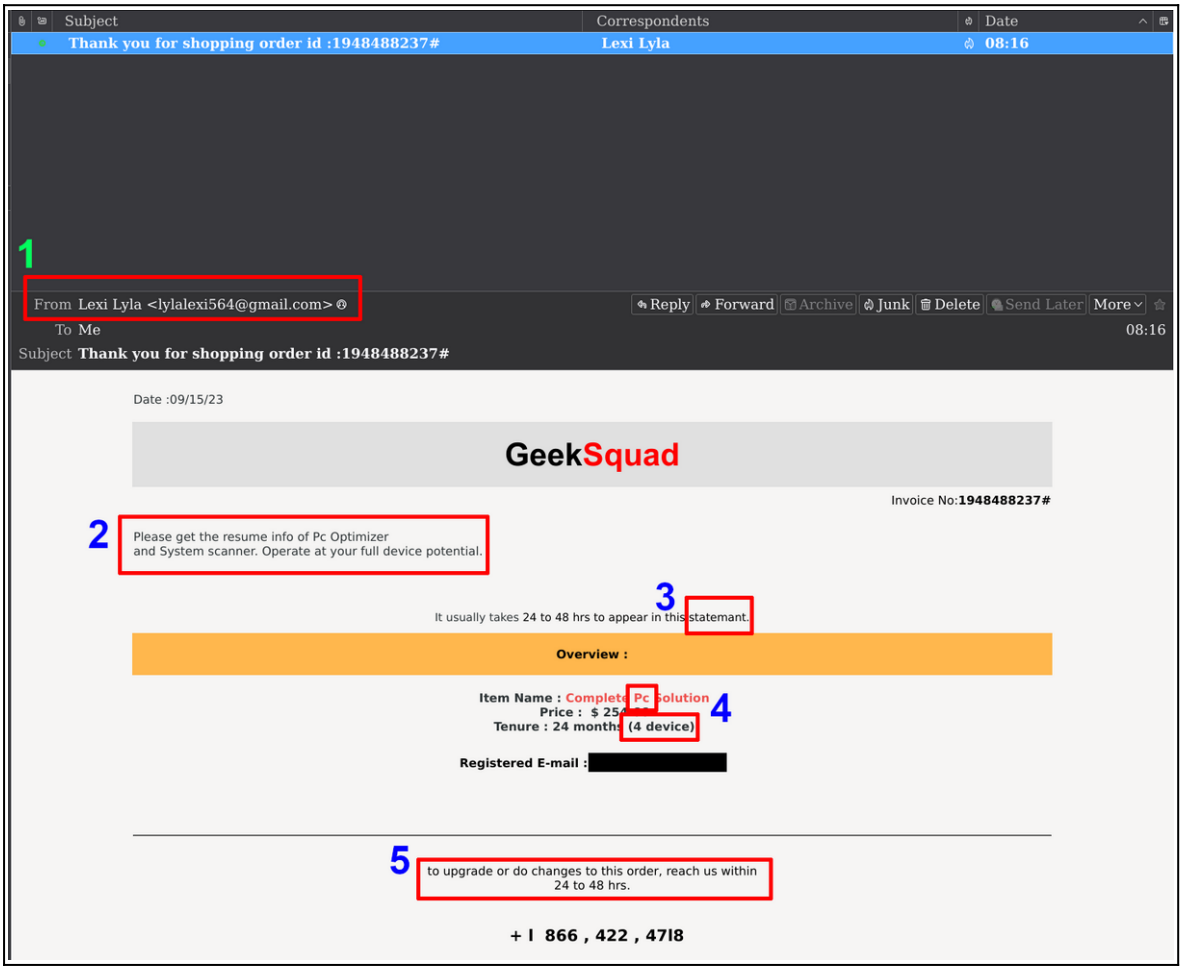
Identifying Bogus Invoice Emails

This is a very common threat that we see almost daily.

It all starts with an email message thanking you for your purchase and providing an invoice, either in the body of the email or as an attachment, similar to the image below:

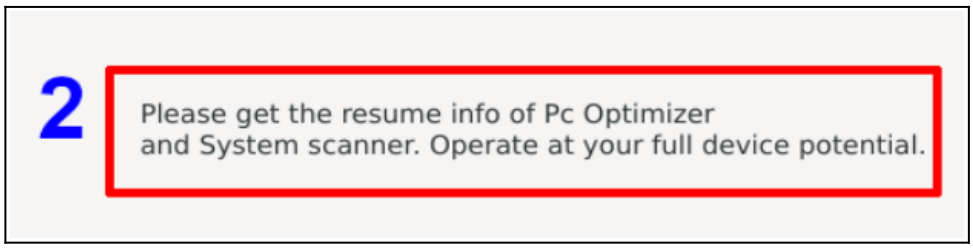


First, NEVER call the phone number provided! They will claim they need to connect to your computer to credit your account / reverse the charge and once they've established a connection they will immediately look for sensitive information that they can steal (like username and passwords for websites, bank account or credit card information, etc.) or they might install additional remote access trojans (RAT for short) that will grant them access to and control of your machine anytime it is on and connected to the internet.

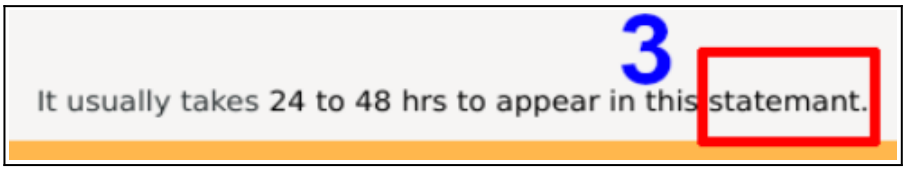
Now, let's examine the clues that should leap out at you if you receive a similar email message.

1. The sender's email address is not from the company that supposedly sent you the "invoice."
    A. You can see in the image above (look at green #1) that the sender is using a Gmail address (lylalexi564@gmail.com.) A legitimate invoice from the GeekSquad would come from BestBuy.com; it definitely would NOT come from a Gmail account.

2. The body of this message is littered with grammatical and spelling errors. I can barely make sense of what they are trying to say in rectangle #2… “Please get the resume info of Pc Optimizer” is so nonsensical it should immediately raise a mental red flag.

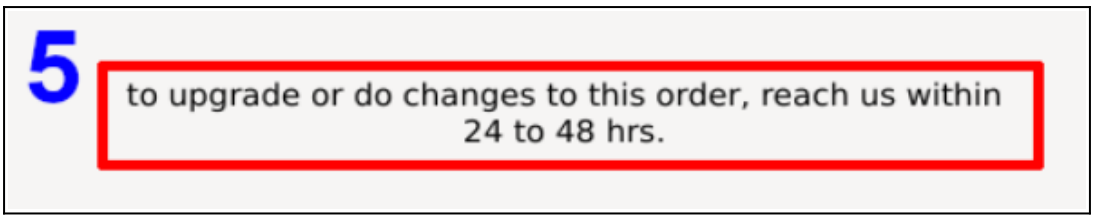


3. The misspelling of “statement” should be another mental red flag.



4. The accepted abbreviation of “personal computer” is PC, not Pc, and using the singular “device” for 4 device**s** is another pair of warning signs.

5. Lastly, the wording used and lack of proper capitalization in the closing should pretty much confirm any suspicions that this entire message is bogus.



This particular example is easy to categorize as bogus, but some of the messages we’ve seen have been very sophisticated and could fool all but the most observant. So what should you do if you receive a similar message without any of the obvious clues discussed above?

First, remember than **any links, attachments, or phone numbers in the message in question should not be trusted.** Treat the message as fake until it is confirmed to be legitimate.

Second, if you have an account with the company for which the invoice claims to originate, log into your account using your established method (personal bookmark, password manager, or simply opening up your web browser and typing in the company website (for example, Amazon.com, McAfee.com, etc.) I cannot stress enough that you should **never use any links in any suspected emails!!**

Once you've logged into your account you should be able to find when your actual subscription renews.

Lastly, if you're an established client of 1Geek4U you can always forward the message to us for review. We have a variety of tools that we can use to verify the authenticity of any email messages of suspicious origin.

Feel free to download this PDF and keep it as a reference.

Surf Safe!