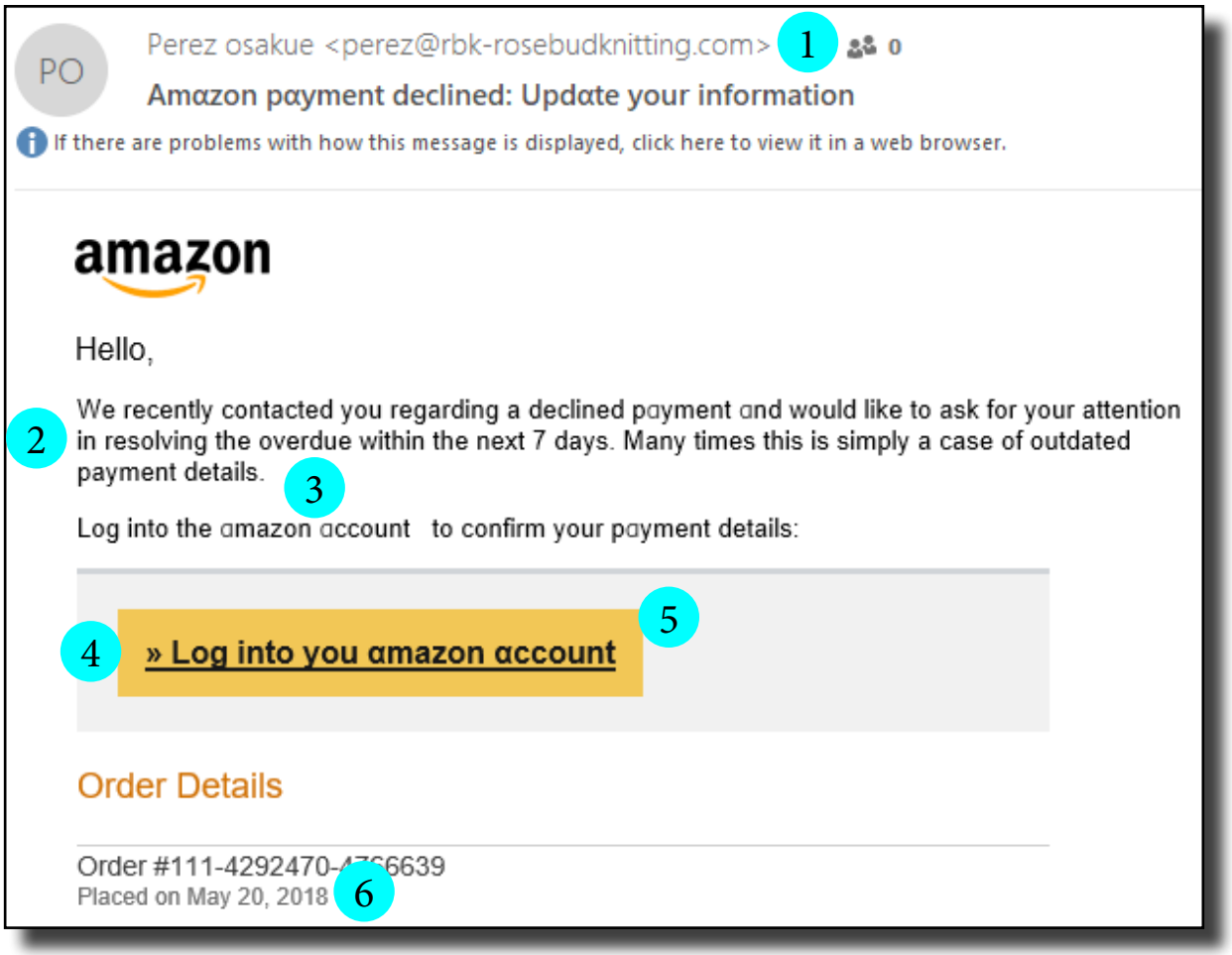
Identifying Scam Emails

1. Take your time. Scammers want you to get worked up so you rush to action without thinking thoroughly.
2. Don't assume that real information is a good sign of legitimacy. A scammer can find your boss's name from LinkedIn or family members from Facebook.
3. When in doubt, sign on -- but NOT through a link in the email. Open up your browser and sign on to Amazon, your bank, your credit card service, whatever. See if there are any alerts.
4. Consult an IT professional or a 14 year old. Both very likely know more about technology than you do, and will be flattered that you want their help.

Email I received from Amazon-ish:



1. Sender's address is suspicious. Mail from an Amazon customer rep is going to have an amazon.com email address. Even email sent on behalf of a third-party seller comes from @marketplace.amazon.com.
2. Bad grammar. Amazon sends out tens of thousands of these boilerplate emails. Someone really does proofread and edit them. And your parents said an English degree wouldn't be worthwhile...
3. Amazon capitalizes the word "Amazon" everywhere it appears in text. It's only the logo that's lowercase.
4. "Log into your amazon account." You bet, Perez, I'll log into me account posthaste!
5. If I hover the mouse over that link (don't click!) I see that the hyperlink would take me to https://katherinesmile.net/ama/amazon.com/amazon. Trust me, Amazon.com hosts its websites at, well, Amazon.com.
6. Sanity check. I received this email on July 25. Would Amazon wait two months on a declined payment? Nah.

These same kinds of flags can be found in other scamming emails -- IRS, your credit card, bank, Etsy payments, anything. No matter what kind of dire emergency the alert seems to indicate, don't click on any links, and don't respond to an email with any personal information or financial info. Contact the actual company or organization in question, then go back to safely enjoying pictures of kittens and puppies on Imgur.