

* The sender’s email address is weird. No legitimate company is going to use this kind of email address.
* For a real threat to security, an email would most likely be addressed to the user’s name. An email sent with a generic salutation is probably going to be sent to large groups of people. This is a good indication of fraud.
* Note the extra space in front of the comma. A professional communication will be grammatically correct. Note that the tone in this email does not sound “on brand”.
* I’ve circled “indefinitely” because there is no legitimate company (especially one in the business of making money, like a Big Bank) that wants to lose business. This is an example of a threat to intimidate recipients into acting.
* This may sound like a pet peeve, but “manner” should be “matter.” It’s another indication that the communication is not being written by a professional.
* See the strange URL? That is a glaring red flag.
* The period at the end should (obviously) not be floating in mid-air.
* The red box is listed because there is no closing signature. Take a look at our emails to members. They all have a format. This format includes a closing signature and contact information. In this example, there is no corporate branding (aside from the logo – something that is easy to Google). A legitimate message should contain corporate colors, website, phone number, and maybe a tagline. All of that is missing.

**\*PRO TIP\*** You can also copy and paste the info (not the link) and Google it. In this case, it brought up (the real) Chase website fraud landing page confirming this is a fake email.