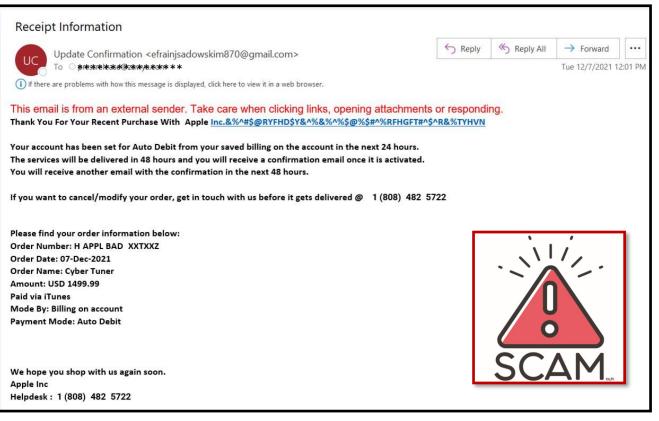
Kathy Papalia, the Diocese of Erie's Network Administrator, sent a warning about email scams and included incredible insights in spotting scams. The following is a screenshot of the fraudulent email and her tips on recognizing that it is a scam.



## How do I know this is a scam?

- Look for odd wording or weird links: There sure are a lot of percentage signs in the web link. And, I doubt Apple would use "Apple Bad" in their order number.
- **Scammers use fraudulent email addresses:** An Apple purchase would come from an official email address NOT a gmail address. I look at email from random gmail accounts as potentially fraudulent.

• Checking email addresses isn't enough: Do your due diligence where phone numbers are concerned. Apple's support number would be a 1-800 number not a 1-808 number. Never dial the phone number in a concerning email. Always confirm the number through independent means. In my case, I googled "Where is the 808 area code" and learned 808 is Honolulu's area code. That is very sneaky because most people see an 800 number and automatically assume it's a toll free business number.

• Scammers use scare tactics: Note the sentence "If you want to cancel/modify your order, get in touch with us before it gets delivered." Don't let THEIR sense of urgency get past YOUR defenses.

• Scammers want your personal information: Scammers are hoping you will call them to dispute the charge. When you do, they'll ask you for your credit card number so they can "research the issue". Or, they'll ask you for your bank account number so they can "reverse the charges". Or, they may ask for your PayPal credentials or even suggest setting PayPal up on your behalf. Since the "charge" supposedly comes from iTunes, they may suggest you purchase an iTunes card so they can credit it with the refund. Once they have your personal information, they will steal your funds.