February 23, 2018

by Ari Lazarus
Consumer Education Specialist, FTC

We've recently heard that scammers are recycling an old phishing attempt. In this version, scammers, posing as a well-known tech company, email a phony invoice showing that you've recently bought music or apps from them. The email tells you to click on a link if you did not authorize the purchase. Stop – do not click on the link. That's the new twist on an old scam.

More precisely, you just experienced a phishing attempt – that is, when a scammer uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information. The scammers then use that information to commit fraud or identity theft.

Scammers also use phishing emails to get access to your computer or network – then they install programs like ransomware that can lock you out of important files on your computer.

Here are some tips to help keep your information secure:

- **Be suspicious if a business, government agency, or organization asks you to click on a link that then asks for your username or password or other personal data.** Instead, type in the web address for the organization or call them. The link in the email may look right, but if you click it you may go to a copycat website run by a scammer.
- **Be cautious about opening attachments.** A scammer could even pretend to be a friend or family member, sending messages with malware from a spoofed account.
- **Set your security software to update automatically, and back up your files to an external hard drive or cloud storage.** Back up your files regularly and use security software you trust to protect your data.

Lastly, report phishing emails and texts by forwarding them to spam@uce.gov and filing a report with the FTC.