



SHIPPING UPDATE SCAM

Scam predators are seeking your personal information in a scam that has escalated with the increased online shopping during the Coronavirus Disease 2019 (COVID-19) pandemic. This particular scam begins with an email or text message that is supposedly from United Parcel Service (UPS) or FedEx. The email states you have an item that is ready to ship but you need to update your shipping preferences, when there is actually no package. If you click on the link or download the attachment, you are likely to end up with malware. Malware is software that damages your computer, cell phone or other device with a virus that allows a scam predator to access your identity and other personal information. Do not let this happen!

The Federal Trade Commission (FTC) and the Better Business Bureau (BBB) recommend the following to avoid any delivery confusion and potential scams:

- ♣ Do not click! If you receive an unexpected email or text message, do not click on any links or open any attachments.
- Enroll yourself on the company website. If you are expecting packages from UPS or FedEx, sign up online so that you can check status and account information for yourself.
- Guard against malware. Keep your software up to date on all your devices. Set your security software, internet browser and operating system (like Windows or Mac OS X) to update automatically.
- Protect your personal information at all times. This includes your full name, address, birthdate, Social Security and account numbers.

Note: You may report scam predators to the FTC, BBB, Adult Protective Services (APS) and the Federal Bureau of Investigation Internet Crime Complaint Center.

If you think you may be a victim of a scam, contact **San Bernardino County APS at 1 (877) 565-2020** or your local police department.