SCAM REPORT

Submitted by Arnold H. Shifrin, Director of Communications, SALT

Package Delivery Scam

How it works: You receive an email or text message from a delivery driver looking for your residence. The driver states he works for UPS® (United Parcel Service), FedEx® Corporation, or the USPS (United States Postal Service) and has a parcel for you, but there are "problems with your shipping address." The message includes a tracking number and the delivery company's logo and graphics, and appears to be authentic. You are instructed to call the driver on his cell phone to re-confirm the delivery and provide directions.

If you call the number, you are asked to verify your name and address. The driver asks for your credit card information to cover a small delivery and handling fee. If you comply with the request and furnish the information, your identity has been stolen. Money will be drained from your account and fraudulent purchases will be charged to your credit card. No parcel will be delivered to you.

If you tell the driver you did not order anything for delivery, you are advised the package is a gift from a relative or friend, so you would not have expected it. The driver is courteous and patient and has a professional demeanor throughout the conversation, making it difficult for you to spot this as a scam.

Instead of calling the driver on his cell phone, you may be asked to click on a link or open an attachment in the message to re-confirm the delivery and provide directions. If you follow these instructions, malicious software is installed on your device, and fraudsters will steal your personal and financial information.

How to protect yourself

- Keep a record of all packages you are expecting, when they are scheduled for delivery, from what companies they were ordered, and their tracking numbers. When you place an online order for delivery, you will receive a tracking number when the vendor confirms the order. Tracking numbers allow you to monitor the movement of in-transit parcels you are expecting and help verify what a carrier's agent tells you about a pending delivery.
- Never provide personal or financial information to unsolicited callers. Legitimate delivery carriers do not charge to "redeliver" a parcel and will not ask for this information.
- Do not click on links or open attachments in unsolicited emails or text messages. If you're not sure whether a message from a delivery carrier is authentic, contact the carrier's customer service department for confirmation. Use the legitimate website address or telephone number listed below, not one that was given to you by someone else.
  - o UPS: ups.com; 1-800-742-5877
  - o FedEx: fedex.com; 1-800-463-3339
  - o USPS: usps.com; 1-800-275-8777
- Before providing any information online, be sure the carrier's URL in your browser's address bar is correct and that it is preceded by a "padlock" icon. The icon signifies the website is secure and the data are encrypted.
- Look for the following signs of bogus carrier websites: misspelled email or website addresses (e.g., fedx.com, fed-ex.com, usps.gov), spelling and grammatical errors, and the excessive use of capital letters and exclamation points.
- Do not conduct online transactions if you are in a public Wi-Fi environment (e.g., library, airport, coffee shop). Individuals nearby may have access to the information on your device.
- If you are a victim of this scam, report it to the delivery carrier and your local police department.

[Sources: FCC,ABC]