How to Identify and Avoid Package Delivery Scams

This is the time of the year (yes… already) when shoppers around the world begin ordering gifts for holiday celebrations. COVID-19 has only increased the need for online shopping, but beware! Delivery scams and package theft become more prevalent around the holiday season.

Many delivery scams start with a text message or an email about delivering a package to your address. These messages often include a "tracking link" that you are urged to click in order to update your delivery or payment preferences. You may also receive a voicemail message with a call-back number, or even a "missed delivery" tag on your door with a number to call.

While these messages often look or sound legitimate, you should never click a link, open an attachment, or call back a number from an unexpected delivery notice. Contact the delivery service or seller directly using a verified number or website.

Here are some additional warning signs of package delivery scams:

- Unexpected requests for money in return for delivery of a package, often with a sense of urgency.
- Requests for additional personal and/or financial information.
- Links to misspelled or slightly altered website addresses, such as "fedx.com" or "fed-ex.com."
- Spelling and grammatical errors or excessive use of capitalization and exclamation points.
- Lack of the padlock symbol and HTTPS in a URL.

Scammers are often very clever and will go to great lengths to deceive you. Be suspicious of any unexpected package delivery notice and report them to your security team.

If you have any questions regarding this tip, please contact Information Security via Mark.Nagiel@SupremeLending.com. Thanks for participating in the information security effort!