Nicolet NATIONAL BANK

SCAM AWARENESS BULLETIN

Real People. Real Conversations.

Online Shopping – Package Delivery Fraud

Introduction

The COVID-19 pandemic is dramatically altering how millions of American consumers shop, with online sales skyrocketing thanks to consumers' concerns about the health risks of shopping in brick and mortar stores. According to the United States Census Bureau, U.S. retail e-commerce reached $211.5 billion in the second quarter of 2020, up 31.8 percent from the first quarter and 44.5 percent year-over-year. With delivery vans buzzing around neighborhoods as never before, scammers are looking to capitalize on this trend.

According to reports from the Federal Trade Commission and the Better Business Bureau, scammers are increasing their use of the fake package delivery scam. In a typical scam of this type, consumers receive a text message, email, or phone call informing them that they have a package waiting for them or that the delivery service (*e.g.,* FedEx, UPS, or USPS) was unable to deliver a package.

To get the package delivered, the consumer is asked to click on a link and "verify" personal information or supply payment information (like a credit card or bank routing number) to reschedule the delivery. In other cases, the scammers' messages may direct recipients to an authentic-looking website (for example, a phishing site that looks like an Amazon customer satisfaction survey). Consumers who fall for this scam can end up inadvertently signing up for difficult-to-cancel subscription services.

These delivery messages can be quite convincing—but they are fake and generated by scammers trying to extract valuable information from consumers. As consumers come to rely more on e-commerce for day-to-day needs, they may be more likely to assume these messages are legitimate. However, with a little knowledge, you can avoid being the next victim of these swindles.

Here Are the Steps to Reduce Your Risk

- Do not click on any links or attachments in text messages or emails claiming to be from a package delivery service. If you receive a phone call from someone claiming to be with a package delivery service, hang up. Do not press "1" (or any other number) to be connected to a representative.
- If you do click on a suspicious link, do not supply any personal information such as your Social Security number, mailing address, credit card number, or bank account routing information, even if it is just to "verify" your identity.
- Do not be alarmed by language in text messages, emails, or phone calls that claim your response is "urgent." This is a common tactic that scammers use to get you to act before thinking.
- If you are unsure whether you have a package waiting for you, go the delivery service's website (*e.g.,* amazon.com, usps.com, or ups.com) and enter the tracking number there.
- If you receive a spam text message, forward it to short code 7726, which sends the message to the GSMA's Spam Reporting Service. This is a service run by the major U.S. wireless carriers to help identity trends in scam texts.

If you suspect that you have become a victim, report it immediately. You can file a complaint at Fraud.org via our secure online complaint form. We'll share your complaint with our network of law enforcement and consumer protection agency partners who can investigate and help put fraudsters behind bars.

References

(1) Scammers capitalizing on online shopping boom with wave of package delivery fraud as found at https://www.fraud.org/package_delivery_alert?utm_campaign=oct_2020_fraud_alert4&utm_medium=email&utm_source=ncl