BankOnITUSA®

INFORMATION SECURITY BRIEF

NOVEMBER 2021

TIPS FOR ONLINE HOLIDAY SHOPPING

With more and more people doing their holiday shopping online, the U.S. Department of Homeland Security has issued some general tips to keep shoppers safe.

Software Updates
Whether shopping from your laptop or tablet, make sure your OS and antivirus software is installed and up to date.

Password Protection
Make sure you don't use the same password for multiple accounts. When possible, use multi-factor authentication.

Avoid Public Wi-Fi
Public Wi-Fi networks are not secure and should never be used to conduct online shopping or banking transactions.

Know Your Vendor
Stick to doing business with established companies you know. Legitimate vendors us Secure Socket Layer (SSL) to protect your information. And when ordering by phone, use only vetted apps from your device's designated app store.

Holiday Phishing Trip

Tis the season for stacking presents at your front door — and being vigilant against holiday scammers.

The Holidays used to be about stacking colorfully wrapped boxes under the tree or in the car on the way to celebrate with family. But these days, a better indicator of the holiday season is the growing piles of brown shipping boxes accumulating at your front door. In many ways, online commerce has made gift-shopping a lot easier for everyone. But the volume of packages arriving daily to your doorstep has also made it easier for bad actors to try and scam you and your customers out of money.

Fraudulent emails and text messages, commonly referred to as "phishing" or "spoofing," are on the rise. They come emblazoned with official-looking logos of legitimate shipping companies, like UPS or FedEx, claiming that one of your packages got lost or misdirected. To schedule a new delivery, all they need is your name, address, phone number, and date of birth. Seeming harmless enough, the scammers then ask for a form of payment to cover a small "redelivery fee."

And once they have you hooked this far, the phishers prompt you to verify your identity with a Social Security number or email address and password. Then they reel you in.

This time of year is stressful enough without having to worry about whether or not Amazon lost Aunt Cheryl's new Yeti or little Josie's coveted Nintendo Switch. To protect your identity and bolster your peace of mind, here are some tips from the shipping companies, themselves, on what to look out for when holiday scammers come phishing:

- **Asking Too Much:** Legitimate shipping companies do not ask for payments, personal or financial information, account or ID numbers, or passwords to deliver packages.
- **Act Now!:** Scammers will often try to get you to panic by insisting that action must be taken immediately. They can also threaten ("your account will be suspended") or try to entice ("you could win a prize") if you don't act soon.

- **Bad Grammar:** A telltale sign of a scam is a message rife with misspellings, grammatical errors, and sloppy design, including use of distorted or pixelated logos. This includes links to subtly (and intentionally) misspelled web addresses.

- **No Callback Number:** Typically, a legitimate shipping company (or, really, any online vendor) will give you multiple ways to get in touch with them, such as a phone number, mailing address, or physical location. When in doubt, always respond outside of the email or text by looking up and dialing the company's number yourself.

If you believe you've received a spoof or phishing message regarding a package, contact the shipping company independently to report the activity. That way, the company can act to thwart the suspicious activity and warn other customers.