ATTORNEYS AT LAW

BULKLEY RICHARDSON

BETTER REPRESENTATION

STAY SECURE ON CYBER MONDAY AND BEYOND

The holiday season is the most wonderful time of year for hackers and cybercriminals. Online shopping and charitable giving can open you up to many dangers, including Cyber Monday scams, ransomware attacks launched over long weekends, email phishing and more. Consider the following tips to keep your finances and networks secure this holiday season.

1. Shopping Scams:

Treat "One-Day Only" promotions that offer huge discounts on brand-name merchandise with a skeptical eye. (**The Ray Ban scam**, which advertises 90% discounts on sunglasses, is one that frequently appears in most social media feeds.) **According to the FBI**, such promotions are frequently scams. If you were shopping in person, you would verify that a store exists or they had merchandise in stock before you handed over a credit card for "something in the back." Do the same online.

2. Phishing, Delivered:

Resist the urge to click on links. That is the easiest way for cybercriminals to find their way into your systems. Fake correspondence about deliveries—**texts** that purport to be from FedEx, **notifications** about a missed delivery, **emails** about upcoming shipping—are rampant. To avoid accidentally compromising your accounts (or subjecting your business to **ransomware**), default to not clicking links. At the very least, confirm that the sender's email address corresponds to the business they claim they are writing from, and hover your mouse over any hyperlinks to determine that the url matches the company before you open it.

3. Misdirected Donations:

This Giving Tuesday, make sure you are giving to organizations that actually exist. One easy way to do this is to look for an organization's tax ID number (searchable on the IRS's website **here**); the FTC **also recommends** searching a charity's name and the word "scam" or "complaint" before giving money. Thank you notes for donations you do not remember making, pressure to give immediately, and suggestions that you make contributions in the form of gift cards, cash, or wire transfers, rather than by check or credit card, are some **signs of potential fraud**.

May your days be merry and bright—and your data security uncompromised. If you have questions about these tips, or want to give yourself the gift of a Written Information Security Program, please contact Lauren Ostberg, **lostberg@bulkley.com**, or any other member of Bulkley Richardson's Cybersecurity Practice Group.

Lauren Ostberg

lostberg@bulkley.com
413-272-6282