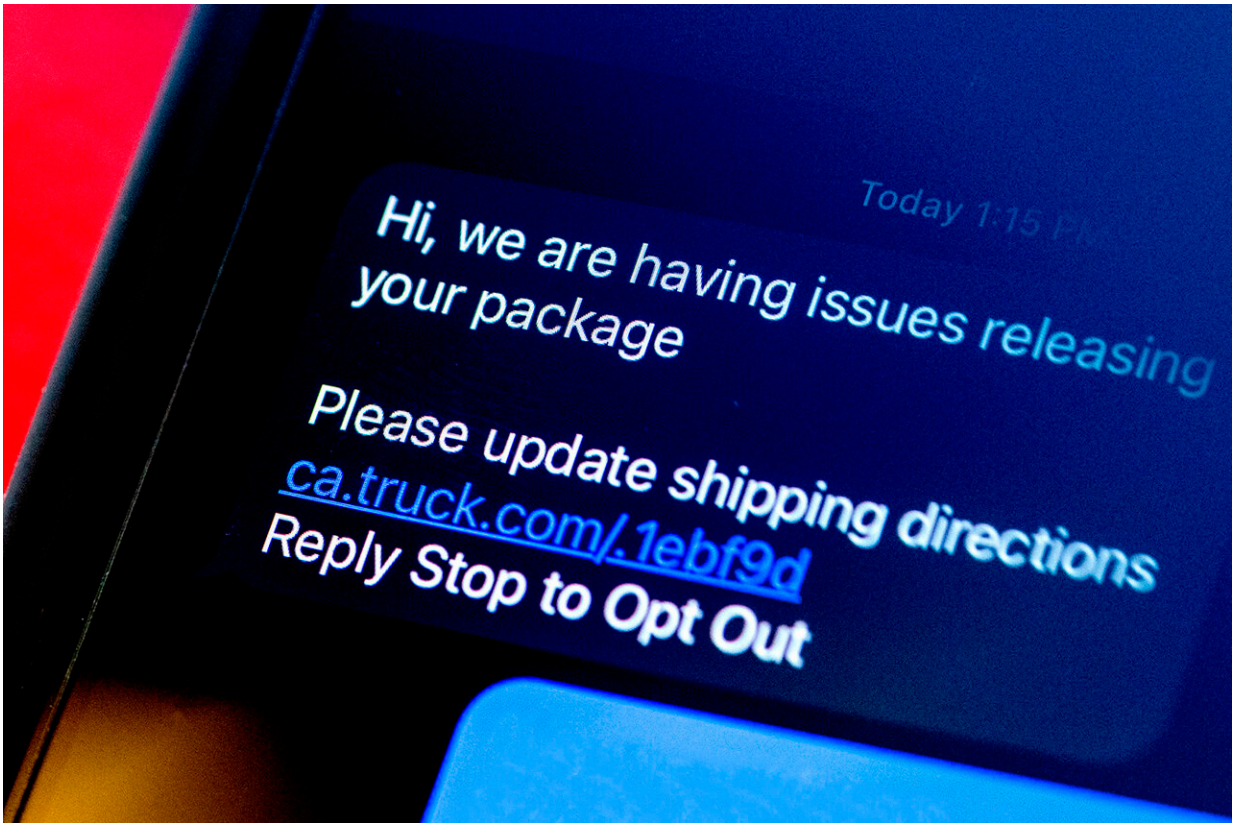
Here's how to stay safe while online shopping for the holidays

December 17 2021, by Molly Callahan



Be on the lookout for unexpected shipping notifications, says computer science professor Engin Kirda. Scammers are betting on an increase in holiday shopping to take advantage of people with fake delivery updates. Credit: Matthew Modoono/Northeastern University

The holiday season is one of the busiest times of year for most online

retailers—and for would-be scammers. While millions of people are searching for that perfect gift, hackers and online thieves will be looking for security vulnerabilities. Here's how to shop smart, and safe, this season.

Around the world, people are expected to spend more than $900 billion in online purchases this holiday season. To make sure none of it ends up in the hands of ne'er-do-wells, Northeastern computer science professor Engin Kirda advises shoppers to stay vigilant.

"We're seeing more and more that people's phones are being targeted, not just their email," says Kirda, whose research includes malware analysis and detection. Cyber-attacks are getting more sophisticated and "harder to detect," he adds.

Be on the lookout for unexpected shipping notifications, Kirda says. Scammers are betting on an increase in holiday shopping to take advantage of people with fake delivery updates.

You might receive a text message from someone purporting to be an online retailer, asking for more information about a recent purchase or delivery. Any other time of year, it would be easier to spot a fake—if you haven't purchased anything from Amazon recently, for example, a text about your package wouldn't make any sense.

But this season, with so many people placing online orders, the likelihood that a scammer hits the mark goes up, Kirda says.

The United Parcel Service advises customers to be on the lookout for fraudulent text messages with shipping notifications. These messages contain what looks like a tracking link, and directs people to a lookalike website asking for login and credit card information. However, officials from UPS and FedEx have said the shipping companies will never ask

for personal or payment information through unsolicited texts or emails.

Kirda's advice? Just don't click any unsolicited links.

"If you get that text message supposedly from Amazon about an issue with your order or your delivery, don't click the link they send. The safest thing you can do is to log on to your account directly and check your order status or call customer support directly," Kirda says.

The deceptive link might send people to a phony website that asks for your username and password, a type of phishing scam that relies upon social engineering, Kirda says. But others can be sneakier—some malware can be activated simply by clicking the link. Then, released upon your device, it searches for security vulnerabilities in the software in the background.

The Israeli tech firm NSO Group designed an incredibly sophisticated piece of malware that is capable of stealing sensitive data from iPhones, all while sitting undetected for months or even years.

The technology presents an interesting research question, Kirda says, but most people shopping this holiday season don't need to worry about this type of security breach; it was designed with political targets and dissidents in mind.

Another popular ploy with holiday shoppers is a gift card scam, which can work two ways. Scammers may try to sell fake gift cards or lure someone into using one to buy a fake item.

In either case, shoppers can avoid falling prey by purchasing gift cards only from well-known and trusted stores, Kirda says.

If you find yourself the victim of an online scam, Kirda recommends

immediately resetting your device and reinstalling all the apps.

"It's a lot of work, but if your device is compromised, the best thing is to do a factory-reset, then reinstall everything," he says. Frequently backing up your phone or other mobile device will make reinstallation smoother, he adds.

Victims of an internet scam should also report it to the Federal Bureau of Investigation's Internet Crime Complaint Center at http://www.ic3.gov, and get in touch with their bank to stop or reverse the transactions.

Provided by Northeastern University