SECURITY-MINDED

Practical security wisdom for daily life.

HOLIDAY SHOPPING HAZARDS

'Tis the season for cyber scams and festive phish

Shopping online can save you time and effort during the often-hectic holiday season, but it also carries risks. While shopping scams happen year-round, attacks tend to surge near the holidays. At this time of year, it's especially important to examine any email that asks you to click a link, download a file, or confirm login credentials or payment information.

When you shop at a brick-and-mortar store, you might leave with a paper receipt, but shopping online usually triggers a flurry of emails, texts, and other communications. People *expect* to receive order confirmations, electronic receipts, and shipping notifications—not to mention countless alerts about special deals, sales, and rewards. Scammers build on these expectations to create convincing phishing emails.

Fake Retail Emails

Scammers often send phishing emails that appear to come from large department stores, e-commerce sites, and other popular retailers. Because consumers already expect to get emails from these legitimate brands, they can fail to notice a well-disguised phish.

Some of these fraudulent emails play on fear. For example, you might receive a fake notification that warns you've been locked out of your online shopping account. It might ask you to verify your identity, in order to steal your login credentials or other personal information. Another common variation uses the lure of free cash or other rewards. Unfortunately, offers that seem too good to be true are often scams designed to steal your money or information.

Return to Sender

Scammers have long used phishing emails that appear to come from shipping services. These phony shipping emails become more frequent during the holidays, and can target both senders and recipients.

Think about it: Nobody wants to experience delays with merchandise they've ordered or packages they've shipped—especially when it comes to last-minute gifts. If you've been shopping online, you're likely to pay attention to an urgent email about a package that couldn't be delivered. These phishing emails use plausible timing and content to trick you into clicking a link or opening an attachment without thinking. They often contain a malicious attachment—perhaps disguised as a fake invoice or notification—that can infect your device when downloaded.

Don't let holiday pressures rush you into snap judgments. It's always better to err on the side of caution.

CYBER-SMART SHOPPING

Share these tips with family and friends:

- **Slow down** – Don't let holiday pressures rush you into snap judgments. Critically examine any email or message that prompts you to do something—visit a website, download a file, or log into an account, for example. If you're not *totally* sure a message is safe, it's always better to err on the side of caution.
- **Stick with what you know** – To avoid falling for online imposters, only interact with trusted websites, preferably those you've used in the past. If you do decide to shop at less-familiar sites, be sure to do your research.
- **Watch for scam sales** – There's a difference between a *great* deal and an *unbelievable* deal. Fraudulent ads and sites may promise luxury goods at very low prices, or the ability to buy a toy or electronic item that's sold out everywhere else. Such purchases could be counterfeit—or never arrive.

What Can I Do?

The best way to avoid holiday phishing attacks is to carefully examine any email that prompts you take action. Since scammers can easily imitate brand logos, "From" addresses, and signatures, you must look deeper.

Ask yourself:

1. Am I sure about where this message came from?
2. Does this message seem odd compared to others I've gotten from this sender in the past?
3. Is this message confusing or does it mention an account or purchase I don't recognize?
4. Is this message urging me to act quickly or trying to frighten me by mentioning problems with an account, purchase, or shipment?
5. When I hover my mouse over the "From" address and web links, do I see anything unexpected or suspicious?

If you're still unsure about an email, confirm the information or offer. Call a trusted number, or visit a known website by typing the address into your browser.

For examples of holiday shopping scams and phishing emails, ask your IT or information security team.

Activity Corner // A Holiday Shopping Story

It was the winter of 1. _____ and my favorite holiday song, 2. _____, was playing on the radio. Before I packed up my family of 3. _____ to head to my 4. _____'s house for the weekend of celebration, I had to do some last-minute gift shopping. I opened my browser to the online store, 5. _____, and picked out the most 6. _____ pair of 7. _____ I could find. Being the savvy and 8. _____ shopper than I am, I looked through my inbox to see if I had any coupons or deals. The first email I clicked on read, "9. _____! YOUR REWARDS ARE WAITING! Click the link below to access your earnings." I knew this email was fake because I had already used these rewards to buy myself a giant 10. _____. After deleting it faster than a 11. _____, I continued to search my inbox until I found another email from 12. _____. The contents of the email seemed trustworthy, but when I hovered my mouse over the "From" address it read, "13. _____ 14. _____ 15. _____@pirate-torrent.com." Another scam from a phony sender! I decided to call a trusted number to uncover any potential savings. While this contact information was legitimate, the deals were not. I eventually ditched the items in my cart, and that was the year I gave everyone in my family a homemade 16. _____ ornament.

1. Year
2. Song title
3. Number
4. Family member (sister, aunt, etc.)
5. Retail store
6. Adjective
7. Article of clothing (plural)
8. Adjective
9. Exclamation
10. Noun
11. Wild animal
12. Same retail store from #5
13. Color
14. Noun
15. Two-digit number
16. Noun