NO PREP

Holiday Scams and Consumer Protection

Phishing, Fake Sales, and Your Rights

Includes: Student reading, case study, differentiated questions, teacher key

Name: Period: Date:

Holiday Scams and Consumer Protection: Phishing, Fake Sales, and Your Rights

Why the Holiday Season Is Prime Time for Scammers

As soon as Black Friday ads start popping up, scammers get to work. They know that in November and

Name: **Period:** **Date:**

Holiday Scams and Consumer Protection: Phishing, Fake Sales, and Your Rights

Why the Holiday Season Is Prime Time for Scammers

As soon as Black Friday ads start popping up, scammers get to work. They know that in November and December, people are shopping more, clicking more, donating more, and rushing more. That combination makes the holidays the perfect time for fraud. When you're juggling school, family plans, and gift lists, you're more likely to skim an email or tap a link without thinking it through. Scammers take advantage of emotions as much as technology. They lean on excitement ("Flash sale!"), fear ("Your package is delayed!"), and guilt ("Don't let a child go without a gift this year"). Their goal is to get you to act fast and think later. That might mean clicking a link in a fake phishing email, entering your card number on a fake website, or donating to a "charity" that doesn't actually exist. The rise of online shopping means more of our purchasing happens through websites, apps, and digital wallets. That's convenient. But it also creates more opportunities for criminals to pretend to be stores, delivery companies, or charities. The good news is that you don't have to memorize every scam. Instead, you can learn the patterns: how scammers normally operate, what red flags to look for, and what rights you have if something goes wrong. Once you see those patterns, the holiday internet looks a lot less mysterious and a lot easier to navigate safely.

How Holiday Scams Try to Trick You

Most holiday scams fall into a few big categories. One is phishing, where scammers send fake emails or texts pretending to be from a trusted company, like a major retailer, a shipping company, or even your bank. A typical message might say, "There's a problem with your order, click here to fix it," or "We couldn't deliver your

package, click this link to reschedule." The link often leads to a spoofed website (a site designed to look real but isn't) that asks for your login, card number, or other personal information. Once you type it in, the scammer has what they need. Another category is fake sales and stores. These might show up as ads for unbelievably cheap electronics, sneakers, or beauty products. The website might look professional, but there are hints: strange web addresses, lots of spelling mistakes, no clear return policy, or only one way to pay (like a wire transfer or sketchy payment app). In the best case, you might get a low-quality counterfeit product. In the worst case, you get nothing at all, and the scammers still have your payment information. Holiday charity scams are a third danger. Real charities do important work, especially around the holidays. But scammers create fake donation sites or spoof the names of real organizations to collect money that will never reach anyone in need. They may pressure you to give immediately, refuse to send written information, or demand payment in gift cards or cryptocurrency. These are two major red flags.

Your Rights as a Consumer: Chargebacks, Agencies, and Complaints

Being careful helps, but no one is perfect. If you (or someone in your family) do get scammed, it's important to know that you're not helpless. In many situations, consumer protection laws give you rights and tools to limit the damage. First, how you pay matters. Using a credit card usually offers more protection than using a debit card, wiring money, or paying in gift cards. If you use a credit card and a charge turns out to be fraudulent or the goods never arrive, you can contact your card issuer and ask for a chargeback: a reversal of the charge. You'll usually need to explain what happened and may have to provide screenshots or emails as evidence, but there is a formal process. With a debit card or wire transfer, the money comes straight out of your bank account and is much harder to recover. Second, there are agencies whose job is to help protect consumers. In the United States, the Federal Trade Commission (FTC) and state attorneys general (AGs) investigate patterns of fraud and can bring cases against companies that break consumer protection laws. While they may not get your individual money back, your report helps them spot large-scale scams and warn others. Local consumer protection offices and Better Business Bureau listings can also give clues about whether a company has a bad history. Finally, you have the right to ask questions before paying. Real charities should be able to tell you their official name, how donations are used, and how you

can verify their status (for example, on a government or watchdog site). Real businesses should provide an address, contact information, and clear return policies. If someone pressures you to act immediately, refuses to provide details, or insists on unusual payment methods, you have the right to walk away. Saying, "I'll check this and get back to you" is a powerful consumer protection tool all by itself.

Smarter Holiday Habits: Check Twice, Click Once

You don't have to live in fear of every email and ad, but you do need habits that make scams harder to pull off. Start with a simple rule: never click on links in unexpected messages about money, accounts, or deliveries. Instead, go directly to the official app or website by typing the address yourself or using a saved bookmark. If the message is real, you'll see the same alert there. Next, get in the habit of checking URLs, spelling, and contact details. Fake sites often have web addresses that are slightly off—extra characters, wrong endings, or strange combinations. They may also have sloppy grammar, generic stock photos, or no physical address listed. If something feels "off," it probably is. For holiday donations, consider choosing one or two reputable charities and going directly to their official websites to give, instead of responding to random texts or social media posts. Talk with your family about how you'll handle donation and purchase requests, so everyone is on the same page. And if something does go wrong, don't be embarrassed—scammers are professionals. Report it, learn from it, and move on. Your goal is not to be perfect, but to be prepared, so your generosity and holiday excitement aren't turned against you.

Case Study Excerpt – "Your Package Is on Hold"

Two days before winter break, Carlos received a text that looked like it came from a major delivery company: "Your package is on hold. Click to confirm your address." He had actually ordered several items online, so the message felt believable. The link opened a page with the company's logo and colors and asked for his full name, address, and card number "to confirm billing." Carlos started typing, but paused when he noticed the web address didn't match the company's official site. He closed the page and opened his real delivery app instead. There were no problems listed. Later, his teacher explained that this was a classic phishing tactic: use a vague but scary message during the busy holiday shipping season to push people into entering sensitive information on a fake site.

1. What specific details in the text and website made the scam believable to Carlos at first?

2. Which clues helped Carlos realize the message was a phishing attempt instead of a real delivery alert?

Multiple Choice

1. According to the reading, phishing scams during the holidays often work by:

   a) Sending messages that create urgency about orders or packages to trick people into clicking fake links

   b) Only targeting people who don't shop online at all

   c) Mailing paper letters that never mention money or delivery but secretly request bank account information

   d) Asking for feedback on a survey with no links or personal information

2. One major advantage of using a credit card instead of a debit card for online holiday purchases is that:

a) Credit cards automatically block all online purchases

b) Credit cards don't require any payments until the next year, so the purchase is interest-free

c) You may have the right to request a chargeback if a charge is fraudulent or goods never arrive

d) Credit cards never get hacked

3. A clear warning sign that a "charity" might be a scam is when it:

a) Encourages you to donate directly through its well-known official website

b) Allows you to think it over and call back later

c) Offers to send written information about its work, finances, and tax deductible status

d) Pressures you to donate immediately and demands payment in gift cards or unusual methods

Matching

Write the letter of the correct definition on the line next to each term.

Term	Definition
1. ___ Phishing	A) Fake site designed to look like a trusted company's page
2. ___ Spoofed website	B) Fake email or text pretending to be from a trusted source to steal information
3. ___ Counterfeit product	C) Reversing a credit card charge when there is fraud or a serious problem
4. ___ Chargeback	D) Agency that investigates fraud and unfair business practices in the U.S.
5. ___ FTC (Federal Trade Commission)	E) Fake or low-quality goods sold as if they were real brand-name products

Fill-in-the-Blank

1. A text or email that pretends to be from a real company and tries to trick you into revealing personal information is an example of _____.

2. A website that imitates a real company's design and logo but is run by scammers is a _____ website.

3. When a credit card company cancels a fraudulent charge and returns the money, this process is called a _____.

Short Answer

Answer each question in 2-4 complete sentences.

1. Using Carlos's case study and the reading, explain why package-delivery messages are such a popular target for scammers during the holiday season.

2. Describe two specific steps a consumer can take before paying to check whether an online store or charity is trustworthy.

3. Imagine a friend admits they clicked a suspicious holiday sale link and entered their card number. Based on the reading, what are two actions they should take right away to protect themselves?