

# 'TIS THE SEASON FOR HOLIDAY SCAMS. LEARN HOW TO PROTECT YOURSELF BEFORE YOU SHOP.



## HOLIDAY SHOPPING TIPS

### **NOW THAT THE HOLIDAY SHOPPING SEASON IS UNDERWAY,**

The National Intellectual Property Rights Coordination Center (IPR Center) wants to remind everyone that all consumers should have an enjoyable shopping experience free from counterfeit or pirated streaming content. Keep reading to learn online shopping best practices, ways to protect financial and banking information, general information to help spot and report fake merchandise, and why digital streaming from unauthorized sites is unsafe.

### **Counterfeit Items**

#### **What's the risk of buying counterfeit products?**

Every year, the United States government seizes millions of counterfeit goods as part of its mission to protect U.S. consumers and businesses. Counterfeit goods cheat consumers with substandard and potentially hazardous products. For example, counterfeit electronics can overheat and explode, bicycle helmets can break upon impact, phony cosmetics and health care products can be made with dangerous or unsanitary ingredients, and seasonal items for the home, like holiday lights, can be poorly wired and cause fires.

Additionally, some of the websites that sell counterfeit goods put shoppers at risk of having their personal and financial data stolen. Online shopping at unknown or unverified sites makes consumers particularly vulnerable to scams that trick them into buying counterfeit and pirated goods.

### **Digital Piracy**

#### **What's the risk of buying stolen products?**

Digital piracy is the illegal copying, downloading, viewing or distribution of copyrighted material via the Internet. It is not a victimless crime when these modern day pirates steal from the artistic talent who create the songs, shows, and movies everyone enjoys. Plus, streaming from unauthorized sites exposes consumers to malware, malicious pop-ups, hacking, and other hazards which could allow criminals access to sensitive personal and financial information. The best way for consumers to protect themselves is to use only legitimate websites and streaming platforms for their digital entertainment. The IPR Center recently launched a series of holiday [anti-piracy PSAs](#) to inform consumers about the many harms they face when viewing pirated movies and television shows.



### **Holiday Shopping DO'S**

#### **Do use one credit card for online purchases**

Consider opening a credit card account for online-use only. Keep a minimum credit line on the account to limit the amount of charges an attacker can accumulate.

#### **Do use good password practices**

- Use a different password for each account.
- Use the longest password or passphrase each system permits.
- Develop mnemonics, or memory aids, to remember complex passwords.
- Consider using a password manager program to keep track of your passwords.

#### **Do be on the lookout for counterfeit, pirated, or stolen goods**

Criminals try to trick holiday shoppers into buying substandard (and often hazardous) counterfeit goods. Look for poor quality, sloppy stitching, missing security labels and irregular markings on apparel. Be vigilant.

#### **Do be on the lookout for counterfeit, pirated, or stolen goods**

Criminals try to trick holiday shoppers into buying substandard (and often hazardous) counterfeit goods. Look for poor quality, sloppy stitching, missing security labels and irregular markings on apparel, as well as prices that are way below what you expect to pay. Be vigilant.

continued

## How Can Consumers Protect Themselves Online?

There are several steps consumers can take to protect themselves when shopping online

- Purchase goods only from reputable retailers and be wary of third-party vendors.
- Read product reviews on websites and research unknown companies and sellers.
- Buy expensive items from the original manufacturer rather than third-party websites.
- Take advantage of security features. Passwords and other security features add layers of protection if used appropriately.
- Take precautions when providing personal information and check published privacy policies to see how a company will use or distribute it.
- Check your statements. Keep a record of purchases and copies of confirmation pages

### Remember

**If a deal seems too good to be true, it probably is.** Criminals use legitimate product photos on their websites, despite selling fraudulent or stolen products. Often, consumers pay full price for subpar items that don't last long. Yet, **one of the biggest dangers illegitimate products pose is that they aren't manufactured or stored properly according to U.S. standards and codes.**

### How Consumers Can Help

Individuals who believe they have purchased a counterfeit, stolen or pirated item can report it by calling the **toll-free tip line** at **866-347-2423, 24 hours a day, 7 days a week, every day of the year**, or reporting it to us by visiting [www.iprcenter.gov](http://www.iprcenter.gov).

### About Us

The IPR Center, working collaboratively with its many public and private sector partners, leads the U.S. response to combat intellectual property theft, counterfeit merchandise, and digital piracy. The IPR Center brings together key federal and international law enforcement partners, prosecutors, academia, and industry experts in a task force setting. By working together, the IPR Center addresses the theft of innovation that threatens economic stability and places the public's health and safety at risk. To learn more about the IPR Center or report the sale of counterfeit goods, please visit [www.iprcenter.gov](http://www.iprcenter.gov).



### Holiday Shopping DON'TS

#### Don't use a debit card for online purchases

Debit cards do not offer protection against identify theft. This is because banks immediately deduct charges from your account and an attacker who obtains your account information may empty your bank account before you even realize it.

#### Don't forget security basics

- Keep your operating system, browser and software up to date.
- Use and maintain antivirus software and a firewall.
- Use caution with email attachments and untrusted links.
- Watch for suspicious activity on your accounts.



**PROTECTION IS OUR TRADEMARK**