In today’s global market, every product is available for purchase at your fingertips—literally! The trend of online shopping has taken the catchphrase, “shop ‘til you drop,” to a whole new level. According to the U.S. Department of Commerce, online spending in the third quarter of 2011 was well over $48 billion. It is estimated that 74% of all Internet users made at least one online purchase during the third quarter of 2011. It is also estimated that in November and December of this year, consumers will spend “$51.7 billion for online purchases, up 15.7% from $44.7 billion for the same period last year.”

Online shopping provides numerous benefits: consumers save a lot of time by not going to the retail store and they have the flexibility and access to research and find the best bargain. But just as pickpockets and carjackers target holiday shoppers, so have online thieves—especially counterfeiters and those selling pirated goods.

The sale of counterfeit products over the Internet—such as fake pharmaceuticals and counterfeit batteries, extension cords, and even holiday lights—could pose a serious risk to consumer health and safety. Sites that sell counterfeit products can pose other dangers for consumers—all too often these sites install malware and some sites even steal credit card numbers and other personal information.

Unfortunately, these websites are often sophisticated and well-designed, and at times hard to distinguish from legitimate sites.

Although it is important to pay attention to the online retailer who is selling a product, consumers should not be discouraged from shopping online. Here are some easy steps you can use to protect yourself this holiday season.

- **If it's too good to be true . . . it probably is.** A product that is selling at a drastic reduction in price is obviously suspicious. Check to see if the site is an authorized retailer (manufacturers often publish these lists). Watch out for sites with poor quality photos; spelling mistakes; logos that look similar, but not identical to corporate logos; and lack of terms of service or contact information. If you are still unsure, ask the retailer for evidence that their products are legitimate.

---

2 http://online.wsj.com/article/BT-CO-20111109-714946.html
• **Insist on secure transactions.** When doing business online, make sure your payments are submitted via Web sites beginning with https:// (the “s” stands for secure) as opposed to http:// (without the –s) and look for a lock symbol at the bottom of your browser. Visit the Federal Trade Commission’s Web site at [www.ftc.gov/privacy](http://www.ftc.gov/privacy) for more information.

• **Check to see if the product has been recalled.** Before completing a purchase, take a minute and visit CPSC.gov or Recalls.gov to determine if the product has been previously recalled. For consumer products, it is illegal for anyone to attempt to sell a recalled product. The U.S. Consumer Product Safety Commission (CPSC) oversees federal recalls, and in order to prevent further deaths or injuries, the agency works to ensure that recalled products are not resold.

• **Beware of counterfeit holiday lights and extension cords.** CPSC recommends that consumers look for the label of a nationally-recognized testing laboratory when purchasing holiday lights and extension cords. Counterfeit lights and cords could have missing or false certification markings, may be mislabeled as to their proper rating, or could have been constructed with substandard components and inadequate safety features. Substandard products may create a fire or shock hazard for your family. Counterfeit products have been the subject of at least a dozen CPSC recalls in the last five years, including various cell phone batteries, circuit breakers, power washer ground fault circuit interrupters, extension cords, power strips, smoke alarms, and conference telephone batteries. These products posed fire and electrocution hazards to consumers.

• **Be certain that replacement cell phone batteries have been certified by a nationally-recognized test laboratory.** Some websites that are not associated with reputable manufacturers and carriers might be selling incompatible or even counterfeit batteries and chargers. Consumers should purchase manufacturer or carrier recommended products and accessories. If unsure about whether a replacement battery or charger is compatible with a particular cell phone, contact the manufacturer of the battery or charger. Lithium-ion (Li-Ion) batteries, which are commonly found in today’s cellular phones, have a lot of energy in a small package and can ignite and explode if counterfeited and not designed and manufactured with standard safety features.

• **Report potential spam and faulty products.** Consumers can play an important role in keeping the market safe by acting as a source of information. If you receive spam that directs you to a suspicious website, report the information to the legitimate company and to the authorities. If you suspect you have purchased a counterfeit or pirated product, notify the legitimate company and contact the place of purchase for an exchange or reimbursement. Report unsafe products to the Consumer Product Safety Commission by visiting their new website SaferProducts.gov or by calling 800-638-2772. Many counterfeit and pirated goods result from complex illegal manufacturing and distributing operations. If you suspect an intellectual property crime, report it to the National Intellectual Property Rights Coordination Center at [http://www.ice.gov/iprcenter/](http://www.ice.gov/iprcenter/) or to local law enforcement.
• **Be particularly careful when purchasing medicine online.** Always consult with your doctor, and only take medications prescribed by your doctor or another health care professional. Use a licensed pharmacy. The National Association of Boards of Pharmacy can tell you whether an online pharmacy is licensed and in good standing. Reputable sites frequently offer toll-free access to registered pharmacists to answer your questions. If you purchase medicine from a new vendor and it does not match the size, shape, color, taste, or side effects of your usual product, contact your pharmacist or the manufacturer to determine if it came from a legitimate source.

• **Once you receive the product, scrutinize labels, packaging, and contents.** There is no foolproof way to know the difference between a bargain and a fake, but labels and packaging can be revealing indicators. Look for missing or expired “use by” dates, broken or missing safety seals, missing warranty information, or otherwise unusual packaging. Check for spelling mistakes and logos that look similar, but not identical to corporate logos.

• **Never click on a link in an unsolicited e-mail.** This is often how spyware and malware spread.

• **Warn friends and family of illegitimate product sources.** Word of mouth is one of the best ways to spread information about dangerous and defective products and those who sell them. By talking about this problem, you may also learn where your friends and family have found reliable, safe, affordable, and legitimate alternatives.

**To learn more about what government and industry are doing to fight counterfeiting and piracy, visit [www.fightonlinetheft.com](http://www.fightonlinetheft.com).**

The U.S. Consumer Product Safety Commission is a member agency of the National Intellectual Property Rights Coordination Center (NIPRC), a federal government task force that uses the expertise of its member agencies to share information, develop initiatives, coordinate enforcement actions, and conduct investigations related to counterfeiting. [www.IPRCenter.gov](http://www.IPRCenter.gov).

The Chamber’s Global Intellectual Property Center is working around the world to champion intellectual property (IP) rights as vital to creating jobs, saving lives, advancing global economic growth, and generating breakthrough solutions to global challenges. [www.theglobalipcenter.com](http://www.theglobalipcenter.com).

# # #