

FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer & Business Education

Holiday Shopping? How To Be On Guard When You're Online

Thinking about shopping for the holidays? It's no secret that browsing and buying online can save you time, money, and effort. The Federal Trade Commission (FTC), the nation's consumer protection agency, says shoppers who stop and think before they click can prevent an online Scrooge from interfering with their purchases and ultimately, their holiday fun.

The FTC and the technology industry recently launched OnGuardOnline, a campaign to help consumers integrate online safety into their daily online routines. The agency says that consumers who take a few precautions when they're online can help minimize the chances of a mishap. Among the tips from OnGuardOnline.gov are:

- * **Know who you're dealing with.** Anyone can set up shop online. Confirm an online seller's physical address and phone number in case you need to get in touch with them. If you get an email or pop-up message from the seller while you're browsing that asks for financial information, don't reply or click on the link in the message. Legitimate companies don't ask for this information via email or pop-ups.
- * **Read between the lines.** Read the seller's description of the product closely, especially the fine print. Words like "refurbished," "vintage," or "close-out" may indicate that the product is in less-than-mint condition; name-brand items with "too good to be true" prices could be counterfeits.
- * **Calculate the costs.** Check out websites that offer price comparisons and then, compare "apples to apples." Factor shipping and handling into the total cost of the order. Then, stack these costs against your budget and needs.
- * **Pay by credit or charge card.** Do not send cash under any circumstances. If you pay by credit or charge card online, your transaction will be protected by the Fair Credit Billing Act. Under this law, you have the right to dispute charges under certain circumstances and temporarily withhold payment while the creditor is investigating. In the event your credit or charge card is used without your knowledge and permission, you generally are liable for no more than \$50 in charges per card. Many companies do not hold consumers responsible for any unauthorized charges made online, and some card issuers may provide additional warranty, return, and/or purchase protection benefits.
- * **Check out the terms of the deal, like refund policies and delivery dates.** Can you return the item for a full refund? If you return it, who pays the shipping costs or restocking fees? Check on when you can expect to receive your order. The law requires sellers to ship items as promised or within 30 days after the order date if no specific date is promised. Can the recipient return your gift? If so, ask that a gift receipt be included in the package.

- * **Keep a paper trail.** Print and save records of your online transactions, including the product description and price, the online receipt, and copies of any email you exchange with the seller. Read your credit card statements as you receive them to be on the lookout for unauthorized charges.
- * **Don't email your financial information.** Email is not a secure method of transmitting financial or personal information like your credit card, checking account, or Social Security number. If you begin a transaction and want to provide your financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some fraudulent sites have forged security icons.
- * **Use anti-virus software and a firewall and update them regularly.** Anti-virus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your account. It scans your computer and incoming email for viruses, deleting them. Your anti-virus software should update routinely with antidotes to the latest "bugs" circulating through the Internet. Firewalls help keep hackers from using your computer to send out your personal information without your permission. Think of a firewall as a guard, watching for outside attempts to access your system and blocking communications to and from sources you don't permit. If your operating system doesn't include a firewall, get a separate software firewall, or install a hardware firewall — an external device that includes firewall software.
- * **Check a company's privacy policy before doing business.** It should let you know what personal information the website operators are collecting, why, and how they're going to use it. If you can't find a privacy policy — or if you can't understand it — consider taking your business to another site that's more security-conscious and customer-friendly.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

November 2005