Safely Buying Prescription Drugs Online: The Comprehensive Guide

THE CANADIAN PHARMACY

www.thecanadianpharmacy.com

Contents

Introduction to Ordering Prescription Medication from Online Pharmacies

In the current economy, people are looking for any way they can to save money on life's necessities. Families are cutting extracurricular activities and buying unbranded at the grocery store, but one product that continues to pose a problem for people on a budget is prescription medication.

For people without prescription drug coverage, those in the so-called "doughnut hole" of Medicare coverage (in which coverage is temporarily suspended until the recipient has paid a certain portion of their drug costs out of pocket), and those who require medications that aren't covered by their current plan, accessing these medications may prove challenging and lead to difficult budget decisions.

One product that continues to pose a problem for people on a budget is prescription medication.

The fact is, when it comes down to either paying the electric bill or purchasing prescription medications, many people choose to cut costs on their medications. This leads to problems with medication compliance and can cause additional unintentional and even dangerous consequences.

For example, using less of a medication prescribed to regulate your heart rate may lead to rapid heartbeat or palpitations. Skipping doses of a medication designed to keep a diabetic's blood sugar in check may cause uncontrollable rises in blood sugar and the associated symptoms. "Saving" antibiotics instead of finishing the course can lead to drug-resistant bacteria and future dangerous infections. In the long run, your additional visits to the doctor's office and the emergency room as a result of an attempt to save money could cost you much more that you ever hoped to save.

Why Do Prescription Drugs Cost So Much?

It's difficult to save money on medications at U.S. brick-and-mortar and online pharmacies. The pharmacies not only have to pay all their staff and the overhead costs of the location, they also have to pay the high wholesale costs to American drug manufacturers and distributors. Wholesale prices on prescription medications in the U.S. continue to climb, and regulations that exist in other countries to keep drug prices low don't exist in the U.S. The drug industry has a powerful lobby, and an overall general resistance to price control allows drug prices to rise with no end in sight. When the U.S. Congress passed an act to reform Medicare in 2004, a section was dedicated to prohibiting the government from stepping in and negotiating lower drug prices.

These higher prices get passed on to you — the consumer — simply so the pharmacies can stay in business

Insurance companies are also common culprits when it comes to higher drug prices at American pharmacies. The insurance plans set a predetermined price that they will pay for each medication regardless of the actual cost of the medication. This price is often less than what a cash-paying customer pays, and, sometimes, the pharmacy actually loses money when filling prescriptions for customers with insurance coverage. They must make up for this by increasing the retail price of the medications — a practice that hits cash-paying customers the hardest.

Why do pharmacies go along with this? They must accept the terms of the insurance company in order to do business with them, and if a pharmacy loses a contract with an insurance company, they run the risk of losing their clientele and money. Unfortunately, the only parties that really benefit from this scenario are the drug manufacturers and the insurance companies.

Saving Money at Your Local Pharmacy

It is possible to save money when doing business with your local pharmacies, but you may have to do some legwork, and your savings may not be as substantial as you would like. Some of the available options include:

- Calling around to different pharmacies to compare prices.
- Doing business with pharmacies that price match against their competitors.
- Choosing generic medications whenever possible.
- Finding pharmacies that offer certain generic medications in three-month supplies for a low price.
- Contacting your drug manufacturer to see if you are eligible for coupons and discounts.
- Filling your prescriptions at pharmacies associated with club stores such as Costco or Sam's Club. These pharmacies typically offer a lower retail price than grocery store or chain pharmacies.

What if you've already tried these methods and your prescription bill is still too high? It might be time to consider online pharmacies.

The Risks and Benefits of Online Pharmacies

Online pharmacies, particularly international online pharmacies, offer opportunities for substantial savings on prescription medications. Why is this?

For one thing, online pharmacies often have a lower overhead. Pharmacists and technicians work together to fill prescriptions in a setting similar to your local drugstore but without a front counter and drive-thru window. Since interruptions are few, the prescriptions can be filled and checked at a faster rate. Patient counseling is done by a dedicated group of pharmacists and physicians, so the pharmacist in charge of checking medications can work uninterrupted, which means that a larger volume of medications can be processed.

Prescription bill still too high? It might be time to consider online pharmacies.

Often, generic versions of medications are available through international pharmacies before they are available through American pharmacies. This can also contribute to huge savings.

The primary reason, however, that buying medications on the Internet is so much cheaper is that online pharmacies can buy medications at bulk prices from the manufacturer, which allows them to pass the savings on to the consumer. International pharmacies can purchase medications from the wholesaler at international prices, which are usually considerably lower than the prices that American pharmacies have to pay. For this reason, medications purchased through international online pharmacies can cost half as much — sometimes even less — than the same medications would cost at an American pharmacy.

Are there any downsides to purchasing medications online? There are a few. You will need to do your research and make sure that you are purchasing your medications through a reputable pharmacy. Unfortunately, many "online pharmacies" are fly-by-night operations looking to make a quick buck selling expired or even counterfeit medications to unsuspecting patients who are looking to simply save money on prescription medications.

Disreputable online pharmacies may also offer to sell potentially dangerous medications — including narcotics — online without a prescription. This opens patients up to the risk of dangerous drug interactions and even overdose. Never do business with a pharmacy that offers to sell you medication without a prescription. Not only is this practice highly illegal, it's also extremely dangerous. Keep in mind that Google and other search engines are neutral parties and do not filter their results. Just because you find an online pharmacy through a reputable search engine does not mean that they are a reputable business, so you'll need to take the initiative to check them out. Also this might sound like a daunting task, it isn't. This guide will provide you with the information you need to determine whether an online pharmacy is reputable or not.

Any time you conduct business over the Internet, you run the risk of your personal information being compromised. This guide will give you step-by-step directions you can use to prevent that from happening. Both the U.S. and Canada have laws in place requiring pharmacies and other healthcare providers to protect your personal health information. In the U.S., this law is called HIPAA, which stands for the Health Insurance Portability and Accountability Act, and in Canada, the law is called PIPEDA, which stands for Personal Information Protection and Electronic Documents Act. Both laws are very specific as to how and when personal health information should be protected and how and when it is allowed to be shared. Doing business with a "rogue" pharmacy not only puts you under the risk of having your personal health information compromised, but you may also be running a risk of having your credit card and other identifying information stolen.

This guide will give you the tools you need to have a safer, more enjoyable online shopping experience.

Understanding Online Shopping

This guide will teach you how to safely purchase prescription medication from reputable online pharmacies, as well as how to identify a reliable online pharmacy versus a "rogue" pharmacy. You'll learn how online shopping works, how to protect yourself from online fraud, and where you can go for more information.

Once you know how to safely browse and shop online and how to identify safe online pharmacies, you will enjoy the savings on prescription medications that online pharmacies can offer!

More people than ever are turning to online shopping to fulfill their needs. Just about anything your heart desires can be found online and delivered directly to your door, often for prices that can't be beat by brick-and-mortar businesses.

Safely shopping online offers speed and savings when buying prescriptions.

A June 2013 article in the Wall Street Journal (http://online.wsj.com/article/SB10001424127887324063304578523112193480212.html) showed that in 2012 alone, online purchases grew by 15 percent and totaled $186 billion. Additionally, a survey conducted by comScore, a data analysis firm, showed that online customer satisfaction is at a whopping 83 percent, (http://stream.wsj.com/story/latest-headlines/SS-2-63399/SS-2-244772/) mostly thanks to the flexibility that online shopping allows and the cost savings consumers can enjoy.

If you've never purchased a product online before, it's reasonable to have concerns and questions. Some of the most common concerns of people who haven't shopped online include fears about computer and credit card security, apprehension about shopping at a retailer that may not be legitimate, and worry about how to handle disputes with online retailers. These concerns are certainly realistic, but honest online retailers have also taken these fears into account in order to provide you with a safe and enjoyable online shopping experience.

How E-Commerce Works

The act of purchasing items online has come to be known as e-commerce, and, as noted above, this method of doing business is exploding.

E-commerce is essentially the same principle as standard commerce — sellers and buyers working together to trade for goods. The only difference is that the trades are conducted electronically through the Internet. Have you ever perused a catalog or seen an ad on TV and then picked up the phone to call the toll-free number and purchase the product? The idea is the same, except that you can find exactly the item you are looking for by going to a website, selecting your item, adding it to what is often called your "shopping cart," and then checking out by entering your credit card and shipping information into a secure form.

Fears and Misconceptions About E-Commerce

Most fears about e-commerce can be boiled down to six basic concerns. Perhaps the most pervasive fear about shopping online is that your credit card and other personal information will be stolen or mishandled. While identity theft is a very real concern, you can mitigate this risk by following some recommended steps to secure your computer and also make sure that you are shopping at a legitimate and trustworthy business. You can learn more about these recommendations in Chapter Three: Securing Your Browsing Environment and Chapter Five: Online Security and Trust Indicators.

Another common concern is that because the business may not exist in a brick-and-mortar location, the item itself may not exist and you may never receive it. Unfortunately, everyone has heard the horror stories about well-meaning buyers being ripped off by scam artists on popular auction or free-listing sites. You can reduce this worry when you are shopping for medication (or anything else) online by only purchasing your products from an online retailer with an actual physical location, a practice that we strongly recommend.

People who are new to online shopping are also often afraid of their information being sold to third parties, leaving them open to spam and other solicitous offers. This is an unethical practice, and carefully choosing the sites you do business with will help prevent this problem. When you are visiting a website you are considering doing business with, look for their privacy policy, terms and conditions, and opt-in options. Sometimes this is provided when you create an account with the website, but it should also be available elsewhere on the website. Use the site's search box to type in "Terms and Conditions" or "Privacy Policy," or scroll down. The information may also be available in the website's "footer." Although many people simply check the box that says that they read the terms and conditions because they are in a hurry, take the time to actually read through and review the information. The site may also automatically sign you up for emails and even regular mail, and this information will be in the terms and conditions wording.

Reputable online pharmacies always have medical and pharmaceutical professionals available for customer support.

One disadvantage that online shopping has over shopping in physical stores is that regular stores allow you to try on or try out a product before you buy it. This is especially a concern when purchasing clothing or electronic equipment. One consequence of this problem is that people today often go to physical retailers, try out or try on the item they wish to buy, and then go online and purchase the product, a practice sometimes referred to as "showrooming." This problem is causing concern for physical retailers who are paying to display the product but are reaping none of the profit.

Many people worry that when buying products online, they will be all on their own with no salesperson to guide them. Most online retailers these days do have customer service representatives available to help you during business hours, and some even provide 24/7 online support. Reputable online pharmacies will always have customer support including medical and pharmaceutical professionals to counsel you.

Finally, consumers who are new to online retail are often worried that they have no recourse if they are unhappy with the product. Just like in the physical retail world, return policies vary from retailer to retailer, so make sure you read the return policy and guarantee before you purchase. This situation is a bit different when it comes to pharmaceutical products however. According to both American and Canadian law, medications that have been dispensed cannot be returned to inventory and resold, so sales through online pharmacies are always final.

The Benefits of E-Commerce

As you may have gathered, online retailers are sensitive to the concerns of consumers, both current and potential, and have taken steps to address those concerns to provide a safe and secure shopping experience. By taking steps to protect yourself as well and conducting business with reputable retailers, you'll be able to enjoy the numerous benefits that shopping online has to offer.

One of the biggest benefits of online shopping — and the reason that most people turn to it for their products — is the convenience factor. You can shop online 24 hours a day, seven days a week, 365 days a year (366 on leap years!). People today are busier than ever, and it can be tricky to get out and get your shopping done in the scant time between leaving work and the stores closing for the night. One online shopping trend that is really taking off is online grocery shopping. More and more grocery stores are now offering this service, as is Amazon through the new program Amazon Fresh. Imagine never having to lug your grocery bags up your stairs again!

Another convenient aspect of online shopping is that you can almost always find the exact product you need. The days of driving all over town looking for the product you want or dealing with cranky salespeople over the phone are gone. A few clicks of the keyboard and mouse and you can find the item you want — even if it's rare — and have it delivered to your door. If you live in a more rural area, this is especially valuable since the product you want may not even be sold nearby.

Online shopping is:

- more convenient

- often cheaper than brick-and-mortar stores

- available 24/7

Securing Your Browsing Environment

Of course, the benefit of online shopping that attracts most people is the lower prices that can often be found online. Since overhead costs (and sometimes storage) are often not a concern, incredible deals can be possible. Online shopping also makes it possible to do business with retailers located outside of the U.S., allowing you to take advantage of local prices that are not affected by pricing regulations or political lobbying. This is especially true when it comes to prescription medications.

Several factors combine to allow Canada and other countries to sell prescription medications for lower prices than in the U.S. The pharmaceutical industry is one of the most profitable in the United States thanks to extensive political lobbying that allows drug manufacturers to raise prices unchecked and even prevents programs like Medicare from negotiating lower drug rates. This results in a drastic difference in the prices of both brand-name and generic medications from other countries — an advantage that online shoppers can use to their benefit.

Securing your browser can keep you safe from most online attacks

Despite consumer fears that shopping online is less secure than shopping in a physical store, the truth is that reputable online retailers have gone to great lengths to ensure that shoppers will have a safe experience. As long as you only shop at retailers whom you have verified to be reputable, you will be safe from fraud. Before you begin searching for an online pharmacy, you should make sure that your computer and your browser are secure. This will not only prevent information about you from accidentally being sent over the Internet, it will also keep other people out of your computer.

Securing Your Computer's Browser

Your computer's browser is your portal to the Internet — the program your computer uses to access the World Wide Web. A variety of browsers are available, with the most popular being Internet Explorer, Google Chrome, Mozilla Firefox, and Safari, which is typically found on Apple products. Each operating system has its own unique advantages and drawbacks, and you may wish to conduct some research of your own to determine which one is right for you.

If you are surfing the Web with an unsecured browser, you may be vulnerable to a number of different issues ranging from annoying pop-up ads to downright dangerous attacks from hackers looking to either steal your personal information or hijack your computer for their own nefarious purposes.

Fortunately, securing your browser is fairly simple, and once this is done, you will be safe from most online attacks. It is important to note, however, that no protection setting is perfect, and hackers are hard at work every day trying to figure out new ways to access and steal your information. In addition to securing your browser settings and computer hardware, you should also be careful to only do business with websites that have earned security certifications and other trust indicators (more about this in Chapter Five: Online Security and Trust Indicators).

Setting Your Browser Privacy

Before hitting the Web, make sure that your privacy settings are on complete lock-down:

Internet Explorer: With your browser open, click the Tools button and then the Internet Options Button, followed by the Privacy tab. Set your privacy level to medium high or higher. Under Location, select the option "Never allow websites to request your physical location." Engage your pop-up blocker.

Google Chrome: To access the privacy settings in Google Chrome, type "chrome://settings/" in your address bar. Under Privacy Settings, make sure that the phishing and malware protection feature is turned on so that you will receive a notification if you accidentally navigate to a questionable site. You should also select the following settings:
- "Keep local data only until I quit my browser."
- "Block third-party cookies and site data."
- "Do not allow any site to show pop-ups."

You may also wish to select the option "Do not allow any site to track my physical location;" however, many sites do use this feature legitimately to provide convenient localization features.

For the best security, you should also disable the autofill option (which automatically enters your username and passwords) and turn off the option "Offer to save passwords I enter on the Web." If you have difficulty remembering your passwords, which is common since so many websites require passwords and have different requirements for those passwords, many tools are available to help including LastPass.com and software like Roboform and 1Password for Mac.

You can also disable Javascript for enhanced security, but more sites are using this coding language and you may limit your browsing experience. Java, although named similarly, is a different technology, and disabling this program won't be as limiting and will increase your level of security.

Mozilla Firefox: Through the Options menu, select the Privacy tab. Select all of the following for optimal security:

- "Use custom settings for history."
- "Clear history when Firefox closes"
- For cookie storage, set to "Keep until I close Firefox."

Check that the following are turned off:
- "Remember my browsing and download history."
- "Remember search and form history."
- "Accept third-party cookies."

Using the Security tab and the Content tab, you should also check the following:
- "Warn me when sites try to install add-ons."
- "Block reported attack sites."
- "Block reported web forgeries."
- "Block pop-up windows."

Safari: Safari and other Mac products are known for their high security and resistance to hacker attacks, but keep in mind that no browser or computer is 100 percent secure from all attacks. If you are using a Mac, you should still take steps to ensure your privacy while surfing the Web. If you are on Safari, click Safari at the top of your screen, next to the Apple logo, and select Preferences from the drop-down menu. From there, choose Security. Turn off "Enable Plug-Ins," "Enable Java," and "Enable JavaScript." Check the box for "Block pop-up windows." Under Privacy, switch to "Always" under Block Cookies.

What Are Cookies?

You may be wondering what all this talk about "cookies" means in terms of computers and browsers, as well as why you want to delete and block cookies. Cookies are essentially small files that your computer automatically downloads when visiting websites. These tiny files store information about the website such as which pages you visited, any preferences you selected while on the site, and even usernames and passwords that you choose for the site.

While cookies can provide a more convenient browsing experience by preventing you from constantly having to select the settings you want or type in your password, the data they store may not be entirely secure. Additionally, some sites use what are known as "tracking cookies" to track where you go once you leave their site. They use this information to send you advertisements more specifically targeted to your browsing and shopping habits. Disabling your cookies will prevent websites and the companies associated with them from following this practice.

Private Browsing

One option to avoid the problem of cookies and other tracking devices is to navigate the web "anonymously" by engaging your browser's private browsing option. This feature is usually easy to turn on and will prevent your browser from storing information about the sites you visit.

Internet Explorer: From the Safety tab on your browser window, select "InPrivate Browsing" from the drop-down menu.

Google Chrome: On your browser toolbar, select the Chrome menu. From there, select "New Incognito Window." This will open a private browser window, and you can surf privately using this.

Mozilla Firefox: From the Firefox menu bar, select File and then click "New Private Window."

Safari: From the Safari tab at the top of your screen, simply choose "Private Browsing" to turn on this option.

Clearing Your Cache

If you don't want to change your privacy settings, you also have the option of increasing your privacy by "clearing your cache." This action removes cookies and login information from your browser after you are done surfing.

Internet Explorer: With your browser open, click on the gear icon to access your settings menu. From there, click "Safety" and then click "Delete Browsing History" on the dropdown menu.

Google Chrome: In Chrome, select your menu icon on the right-hand side of your browser toolbar. Click "Settings" and then select "Advanced Settings" at the bottom of your settings menu. Under the section labeled Privacy, click on the button labeled "Clear Browsing Data."

Mozilla Firefox: Click the Firefox menu in the top left-hand corner. On the menu that pops up, select "History" and then click "Clear Recent History" from the drop-down menu.

Safari: With Safari open, click the Safari menu at the top of your screen and then click "Empty Cache."

Securing Your Computer

Keeping a secure browser while navigating online is important, but securing your computer itself is the second important step in protecting yourself while online. If your computer is turned on, it's connected to the Internet, even if you aren't currently sitting at it. Anytime your computer is connected to the Internet, it is vulnerable to attacks from hackers.

Like securing your browser, there is no way to 100 percent guarantee that your computer is safe from attack. However, like any other criminal, hackers prefer easy targets, so if you make your system unattractive and difficult to attack, a potential hacker is more likely to move on.

Firewalls

Your biggest point of protection for your computer will be your firewall. Firewalls can be either hardware- or software-based. Many computer operating systems (usually Microsoft Windows for PC and Mac OS for Macs) have firewall programs built right into their software, and it's just a matter of making sure that these are enabled.

If you are running Windows on a PC, your firewall is likely already enabled. To check, go to your computer's Control Panel and select "Security." From here, you can access the Firewall. You will be able to see if it is turned on or off. If it is off, you can click to turn it on. This may require an administrator password.

If you are on a Mac, you can access your firewall by clicking your Apple icon in the top left corner of your screen, choosing System Preferences and then selecting the Security icon and choosing the Firewall tab. This page will tell you the current status of your Firewall and give you an option to change it.

Depending on your Internet service provider, you may also have a firewall built directly into your wired or wireless router. You can call your provider to verify this.

Anti-Virus Software

Anti-virus and anti-malware software are programs that you can download onto your computer. These programs run in the background and constantly scan your computer for viruses and other programs that can harm your computer or spy on your activities. When they find a program of this nature, they will notify you and may disable the program automatically.

Because anti-virus software is a simple solution to protecting your computer, some scam companies have created and now market "software" programs that purport to protect your computer but actually download harmful software onto your computer themselves. Never click on any banner or pop-up that is telling you that your computer is infected or needs to be cleaned. If you aren't sure, close your browser completely. If your anti-virus software is genuinely alerting you that an update is needed, the message will display even when you are not online. Watch out for pop-ups that display behind your main browser window as well since those will remain when you close your browser window. Make sure to close these as well. Ideally, if you've disabled pop-ups as seen above, this will not be an issue.

Only use known and trusted anti-virus programs such as Norton, McAfee, Microsoft, and Kaspersky. Free and low-cost anti-virus options are also available from trusted vendors such as Microsoft Security Essentials, AVG Antivirus, Avast, Avira, and Bitdefender. As mentioned, do not click on ads on websites or in pop-up windows for anti-virus programs. Only go directly to the website of the program you wish to purchase and download it. If you purchased your computer recently, you may also still have a trial anti-virus program subscription available since these are often included in your purchase package.

There are many great anti-virus programs that are available for free

If you do happen to pick up a virus, pull up your anti-virus software and have it scan and clean your computer. If this doesn't work, it may be necessary to restore your computer to its original factory state and then reinstall the software and restore your files from a backup source. Keeping backup files is a smart move for this reason. Make a plan to occasionally save your documents, photos, and other important files to a CD or flash drive. For this reason, you should also keep the copy of your operating system software that came with your computer. If you aren't comfortable with this process or are unsure how to do it, contact a local trusted computer professional to assist you.

Updates

When it comes to browser and computer security, it's important to maintain your vigilance. It's not enough to update your settings once and download protective software; you have to continue updating.

Hackers are constantly trying to look for new ways to break into computers, and the developers of protective software are working just as hard to keep up with them. This means that occasionally your anti-virus software or the protective program built into your operating system will need to update.

You can update your system and your software manually, but it can be easy to forget, and this leaves you open to attacks from new viruses. Whenever you have the option for automatic updating, choose this to simplify your life and better protect your computer.

Finding and Verifying Online Pharmacies

Keeping yourself safe when purchasing medication online involves two basic requirements. Now that you know how to keep yourself safe on your end by increasing security on your computer, it's time to look at the second part of keeping your information safe — choosing a legitimate and trustworthy pharmacy.

What's the best way to find an online pharmacy? You could simply type "online pharmacy" into a search engine like Google, but that's not the method we recommend. Unfortunately, at the time of the writing of this guide, the results are just as likely to contain scammy "rogue" pharmacies as they are to show you legitimate pharmacies.

You should always verify that an online pharmacy is properly licensed and follows the standards laid out in this guide.

The better way to find a safe pharmacy to do business with is to look for online pharmacies that are licensed and certified by the appropriate regulatory authorities based on their location. For example, online pharmacies in the U.S. are licensed by the department of health of the state in which they are located and are regulated by the Food & Drug Administration. Canadian online pharmacies are a perfectly viable, safe, and regulated option as well – and usually cheaper than even online U.S. pharmacies. Although they are outside the jurisdiction of the U.S. Department of Health and the FDA, Canada has its own regulatory agencies to ensure the safety of the medications that are dispensed.

For Canadian online pharmacies, one good place to start is the website of a regulatory authority like the Canadian International Pharmacy Association, www.cipa.com. This website offers a link to a listing of member pharmacies so you have a good starting point for your search. You can also find a listing of rogue and fraudulent pharmacies so that you know which companies to avoid.

Is Your Online Canadian Pharmacy Legitimate?

Use this checklist to determine whether the online Canadian pharmacy you have chosen is legitimate and safe:

- A verifiable license from a Canadian regulatory authority is available on their website.
- The pharmacy should have a brick-and-mortar location that can be verified.
- The pharmacy must require that all patients present a valid prescription provided by a licensed physician.
- A phone number that patients can call for assistance with ordering or questions about their medication should be available. Experienced licensed pharmacists should be available regularly to answer questions and provide counsel to patients.
- A full range of medications should be available through the pharmacy, not just popular "lifestyle" drugs such as impotence drugs and weight-loss drugs or narcotic painkillers.
- The pharmacy should never inundate you with spam or other unsolicited marketing.
- The pharmacy should comply fully with the Canadian PIPEDA regulations, which are similar in scope to the U.S. HIPAA law. This information and the pharmacy's policy should be stated clearly on their website.
- All fees and services should be clearly displayed with no hidden fees or other charges.

• The pharmacy's website should be free from sensational announcements promising a new or quick cure for serious diseases and disorders.
• Information about where the pharmacy procures the medications they sell should be available and transparent for the patients. Notifications about recalls and other drug warnings should be provided to patients.
• Patients should receive printed counseling for their medications with the option of further one-on-one counseling with an experienced and licensed pharmacist or physician.

Am I Dealing With a Rogue Pharmacy?

Some rogue pharmacies take careful steps to appear legitimate but are often given away by simple mistakes. If you are doing business with a pharmacy that engages in any of the following practices, stop your transaction and look for another pharmacy:

• The pharmacy is either not licensed or listed by a regulatory agency, or does not display a license number on their website.
• The pharmacy exists only online and does not have a verifiable physical location.
• The pharmacy appears to be new with no track record or patient reviews available.
• A Canadian pharmacy is not listed on the CIPA's website or any of its province counterparts.
• The pharmacy does not inform you about where they purchase your medications or what you can expect them to look like.
• No phone number is available.
• Counseling is either not offered or is done by someone other than a licensed and experienced physician or pharmacist.
• The pharmacy does not require a prescription written by a licensed U.S. physician or provides a "prescription" based on a questionnaire. "No prescription required" is often stated on the websites of rogue pharmacies.
• Only popular weight-loss or impotence medications, narcotics, benzodiazepines, and other highly regulated medications are available through the pharmacy.
• The pharmacy sends you unsolicited spam, print mail, or other marketing materials after you visit their website.
• The pharmacy and its website advertise "amazing" results, "new" cures, and other promises that appear to be too good to be true.
• Additional, unstated fees are tacked on to your purchases.

Online Security and Trust Indicators

Now that your computer and browser are secure and you know some of the ways to identify legitimate pharmacies, it's time to learn about the final step in making sure that you are shopping safely online.

Legitimate sites will keep your personal information private by using secure connections and obtaining certifications to prove that they are using your information responsibly.

Security Certifications

Certain online companies will certify websites that are dedicated to keeping your information private and secure. VeriSign by Norton is perhaps the most famous of these, and you may have noticed their logo on highly reputable sites such as PayPal and eBay. Other well-known security certifications and trust seals include McAfee, BBB Accredited, TRUSTe, Safety Check, Thawte, Trustwave, Geotrust, and Comodo. Online pharmacy trust seals to look for include CIPA, MIPA, PharmacyChecker.com, HealthPricer.com, and (in the U.S. only) VIPPS.

Trust seals and SSL certificates verify different aspects of a websites' trustworthiness and security. Trust seals are awarded by companies that verify that the business is who they say they are and that they are meeting a standard set by the awarding company for good business practices. Companies awarding trust seals do not verify the technical security of the website.

SSL certification is awarded based on the actual technical security of the website. The certifying company will test the website in question prior to certification to ensure that a certain level of safety and security is achieved, usually through encryption of private information. The certification company verifies that the company seeking certification is in fact who they say they are and that they are conducting business in the manner they describe.

Your web browser can recognize an SSL connection and might turn your address bar green.

If you'd like to know the standards set by the awarding agency, you can click on the seal to see more detail. If the image of the seal is not clickable, this is an indication that the image has been copied off the Internet and is not a legitimate certification. This is a common practice of shady websites.

SSL Connections

When a company has been verified, they will use an SSL connection to indicate that you can trust your information to the company. It will also ensure that the data you entered will be encrypted and inaccessible by anyone. SSL stands for "secure sockets layer" and identifies specific protocols have been set to ensure your information is not visible to any "bystanders" who may be on the connection.

Whenever you are asked to enter personal information, from your medical history to your credit card number, you will need to check that you are on a secure connection.

In the address bar of your browser, you will notice that the first four letters displayed are typically “http.” These letters are then followed by the Web address of the site you are on. When you enter a secure area of the website, these letters will change to “https.” The “s” indicates that you are in a part of the website with an SSL connection.

Another way to identify that you are using a secure connection is with a lock icon that may appear in the address bar or at the bottom of your browser. This will depend on the type of browser you are running, as well as the version you have. Some sites may also show a pop-up window or run a temporary page to let you know that you are now moving to a secure area of the website. \

Certification Warnings

Occasionally, you may navigate to a site and have a box pop up with a warning about the site’s security certification. The warning may say the site is self-certified, the certificate cannot be verified, or the certificate is expired. What do these different warnings mean?

A self-signed certificate is an SSL program the site owner can download that will encrypt personal information and allow the address bar to show https. Because the certificate has not been verified by a third-party vendor, you have to trust the website is what it claims to be and that the owner is honest. It’s safer to stick with third-party verified websites when you are giving out health and financial information.

An agreement between a website and a third-party verification company is a business transaction, and the website must pay the verification company for the service they are offering and the privilege of certification. If the website fails to provide payment for the service or lets their agreement with the certification company lapse, their certificate will expire, triggering a warning when you try to navigate to a part of their site that was once certified secure. While this could simply be an oversight on the part of the website, you should be aware that there’s no longer a guarantee that your information will be secure.

In some cases, the problem may be between your browser and the site that issued the certificate. When this occurs, you will be given the option to view the certificate and either continue to the site or turn back. Your information is not guaranteed to be encrypted and secure in this situation.

Email From Pharmacies

You're probably familiar with "junk mail." Any time you sign up for discounts from a business or participate in another type of promotion, you open the door to receive advertisements and other mailings. Although you may think of them as a nuisance, targeted mailing lists are an effective tool for businesses to communicate directly with their customers, and in many cases can be informative and valuable, often containing information about deals and even coupons that are only available to members of the company's mailing list. Unfortunately, some businesses participate in the rather shady tactic of selling their mailing lists to other companies, which is why you may find yourself receiving mail from companies you've never done business with.

What Is Spam?

Spam is the online version of junk mail. Although many people refer to any regular mailing from a business that comes into their inbox as spam, spam is mailings from businesses that come completely unsolicited. Please note that if you signed up to receive discounts or a newsletter from a company, this is solicited mail and is not considered spam.

The ability to mail people through the Internet for free is a fantastic convenience that has revolutionized the way we communicate. Unfortunately, it has also revolutionized the way that shysters get their products in front of consumers who likely don't need or want the product in question. For no cost at all, unethical business owners and scammers can flood the inboxes of unsuspecting victims with emails offering get-rich-quick schemes, services that may not be completely legal, and sham products.

Spam emails do not come from legitimate U.S. or Canadian pharmacies, and should not be opened.

Spam has been used to allow scams that should have died out quickly to proliferate and continue. Sadly, people who are not well-versed in spam still fall for these scams and lose money. One classic spam scam is the "Nigerian prince" trick in which the recipient receives an email from a so-called "Nigerian prince" who is offering the victim a significant portion of his riches if they will allow access to their bank account to store the riches while the "prince" is in exile. Instead of becoming rich beyond their wildest dreams, the victim instead finds their bank account completely cleaned out. This particular scam is still alive and well today in a variety of different forms but with the same basic concept.

Pharmacy spam is particularly rampant, unfortunately. If you have an email address, you've likely received links advertising Viagra, Vicodin, and similar medications for extremely low prices and without a prescription. These unsolicited emails are not coming from legitimate U.S. or Canadian pharmacies although they often use names that are identical or similar to legitimate pharmacies. They may also use logos that are stolen off the Internet or modified to appear legitimate. Additionally, they may link to fake regulatory agencies, for instance, the non-existent "American Drug Association" or "Canadian International Drug Association." This spam typically originates from countries outside the U.S. Russia is a common originating country for this spam as are many Asian countries. If you receive unsolicited emails from pharmacies, we recommend that you delete them immediately without even opening them.

Why Am I Getting Spam?

You may be receiving spam because you signed up for a mailing list of a company who participates in list sharing or selling, or you may be the victim of a spammer who took the time to troll the Internet looking for email addresses of people who comment on forums. It can often be difficult to know.

What Is Phishing?

Spam is annoying, but phishing can be disastrous. This technique is used to steal passwords and other important information (like bank account numbers) from unsuspecting victims. Phishing can happen over the phone, but it's easier for the scammer to use the Internet and email for their criminal purposes.

The most common type of phishing is done by spoofing legitimate sites. Often, the phishing attempt begins when the victim receives an email that appears to be from a legitimate agency, such as the IRS or the victim's banking institution. The email will usually say something like, "We have found a problem with your account. Please follow this link and enter your password to confirm that your account information is correct." When the victim clicks the link, they are taken to a site that mimics the appearance of the legitimate agency. Unfortunately, it's set up simply to collect the information that allows the criminal to steal your identity or the contents of your bank account.

Legitimate Communication or Phishing Attempt?

Financial institutions and other legitimate agencies will never ask you to click a link in an email or enter your password. For instance, the IRS states quite clearly on their website that they never initiate contact with taxpayers via email or any other electronic communication.

If you do receive an email from your bank or other agency requesting that you follow a link or submit your password, assume it is a phishing attempt and do not click the link. If you aren't sure, go directly to the agency in question's website by typing their URL in the address bar and check your information that way or call the agency directly.

Many agencies request you forward emails containing phishing attempts to a specific fraud-alert email address so they can notify customers who may have been affected and attempt to track down the criminal in question and shut down their operation.

Am I on a Spoofed Site?

A "spoofed" website is one that is designed to look like a legitimate site but is actually set up for the sole purpose of stealing your financial information or your identity. Sites that are commonly spoofed include banks, credit unions, insurance companies, and the IRS.

On the surface, spoofed websites look like the real deal, but there are a number of ways to tell the difference:

- The URL address looks slightly different and may include a typo or a .net or .biz instead of .com, .gov, or .org at the end.
- You may spot typos or grammatical errors on the website.
- A webpage with a form requiring you to enter personal information does not have the signs that identify it as secure (see Chapter Five).
- The font or the color scheme may look different than you are used to.
- You are immediately asked for detailed information such as your password, bank account number, or Social Security number before you are able to access the site.

If you suspect that you are on a spoofed site, close the window immediately. If you have already typed in some of your personal information, contact the agency or company right away by phone to notify them that your personal information may have been breached and to create a new password.

How Can I Avoid Spam and Phishing Email?

The best way to avoid winding up on spam and phishing mailing lists is to be very careful whom you give your email address to. Before providing your address, check for a notification that your email address will not be sold to another company. Don't sign up for contests online unless they are being run through a trustworthy brand. Otherwise, you may be unknowingly participating in a scheme to get your email address and sell it to spammers.

If your email provider offers a spam filter, use it. Many services, such as Gmail, offer spam filters as a matter of course and have them automatically set. Check your spam filter periodically to make sure that important information is not mistakenly being routed to the folder. If your email provider does not offer a spam filtering service, consider switching to one of the many free services that does.

Never trust a link in an email unless you are absolutely sure you know who sent it. Even then, be careful. A common phishing technique that is gaining popularity is spoofing email addresses. If you receive an email with nothing but a link in it, especially if the link is nothing but numbers and letters and doesn't indicate where it goes, do not click the link — even if you think you know the person who sent it. If necessary, call the person who sent it to make sure it's safe.

Be careful when visiting forums, message boards, and other chat sites. Don't disclose your email address. Spammers use software that can scan these types of forums and pick out the email addresses to add to their list.

Although it may seem counterintuitive, never click on the unsubscribe links that are often included in spam emails. These links may download a virus onto your computer or may confirm to the spammer that you are likely to click links in spam, therefore identifying you as a prime target. Remember that when you are dealing with a spammer, you are dealing with someone who is not likely to be ethical in nature and probably has no qualms about lying. It may be helpful to set up a secondary email address for conducting business transactions or signing up for email lists. By doing this, you don't risk compromising your primary email address.

Where to Go for Help

Hopefully, you're excited about the prospect of saving money by purchasing your medications online.

However, you may still have some questions about finding a safe and legitimate pharmacy to use—one that you can trust to send you authentic medications and keep your personal information private.

You have plenty of support on your side to help you navigate your way through these waters. Many organizations are working hard to ensure that you are able to get safe, affordable medications from online pharmacies. For more information and advice, we recommend you visit the websites of these organizations.

Consumer Organizations

The Better Business Bureau — www.bbb.org

Perhaps one of the most famous consumer organizations, the Better Business Bureau logs information about businesses in both the United States and Canada. They have set Standards of Trust that they use when evaluating businesses to determine whether they qualify for accreditation, and they continuously monitor companies for compliance with these standards.

Additionally, the Better Business Bureau is the place to go to report complaints and scams. They investigate these reports and make a ruling as to whether the complaint was founded or unfounded. You can search businesses (including online pharmacies) by name to see whether they have Better Business Bureau accreditation and also see any history of complaints.

PharmacyChecker — www.pharmacychecker.com

This independent rating company uses its own system of checkpoints to determine whether online pharmacies meet a set of standards, including:

- Dispensing through a licensed pharmacy
- Keeping personal information secure
- Promising to keep personal information private
- Requiring a prescription
- Providing a verifiable phone number and address

A pharmacy that meets all of these criteria will earn a 5-Check rating from PharmacyChecker. Additionally, the company also provides a place for consumers to leave reviews and ratings of pharmacies.

eDrugSearch — www.edrugsearch.com

Like PharmacyChecker, eDrugSearch is an independent company that collects and compiles information about online pharmacies. They give a star-based rating of one to five stars depending on the pharmacy's adherence to principles along the same lines as PharmacyChecker. Pharmacies do have to pay for a listing on eDrugSearch, however, so be aware that not all genuine pharmacies may be listed on this site.

Patients can also leave reviews about pharmacies on eDrugSearch.

Pharmacy Organizations

In both the United States and Canada, pharmacies are licensed by independent organizations. In the U.S., pharmacies are licensed and inspected by each state's Board of Pharmacy, which is a division of the state's Department of Health. You can check with the Board of Pharmacy website in each state to learn the status of a facility's license and even file a complaint against a facility or an employee.

When searching for online pharmacies in Canada that serve international clientele, you will want to check with two organizations that accredit online and international licensed pharmacies—the Canadian International Pharmacy Association and the provincial international pharmacy association in charge of overseeing the pharmacy.

The Canadian International Pharmacy Association – www.cipa.com

The CIPA provides accreditation to pharmacies serving international clients. The association was founded in 2002, and CIPA members maintain perfect safety records. (http://www.cipa.com/about/) All CIPA-certified pharmacies must adhere to a strict list of rules, including:

- Always requiring a valid prescription from a licensed physician
- Refusing to sell controlled medication
- Protecting patient privacy
- Never sending unsolicited spam or selling email addresses

The CIPA also allows both U.S. and Canadian consumers to file complaints about online pharmacies.

Because CIPA certification is such a desired quality when purchasing from online pharmacies, some rogue pharmacies have copied and pasted the logo to use fraudulently on their own sites. Before doing business with an online pharmacy, visit the verification page of the CIPA website at www.cipa.com/verify-pharmacy/ and check for yourself to make sure that the pharmacy is in fact CIPA certified.

International Pharmacy Association of British Columbia — www.ipabc.ca

Manitoba International Pharmacists Association — www.mipa.ca

The International Pharmacy Association of British Columbia and the Manitoba International Pharmacists Association are the provincial international pharmacy associations that provide accreditation to international online pharmacies in addition to the accreditation provided by CIPA. The pharmacy's website should state which association they are affiliated with, but you should still verify this through the website of the association.

Government Organizations

Unfortunately, the U.S. FDA has not embraced international pharmacies. While they regularly take action against rogue pharmacies, shutting them down, and seizing millions of dollars worth of illegal and counterfeit medications, they have chosen to lump legitimate online pharmacies in with the rogue pharmacies. They claim that U.S. citizens who use any online international pharmacy—even those fully accredited by independent organizations and dedicated to protecting patient safety—are at risk for purchasing counterfeit or unsanctioned medications.

Despite these dire warnings from the FDA, the truth is that there are no reported incidents of a patient receiving a counterfeit or unsafe medication from an accredited and legitimate online Canadian pharmacy.

Health Canada — www.hc-sc.gc.ca

Health Canada is Canada's federal department of health. Their website contains important information for American consumers.

One of the most helpful features of the Health Canada website for consumers looking to purchase medication online is Canada's drug product database (http://www.hc-sc.gc.ca/dhp-mps/prodpharma/pdl-ord/pdl_list_fin_ord-eng.php), which allows you to determine whether a medication being offered by a purported online Canadian pharmacy is actually a real and legal medication or if it is possibly a counterfeit. You can also look up Canada's requirements and regulations for advertising to determine whether the pharmacy you are considering is following the law.

What to Do If Things Go Wrong

If things do go wrong, you still have options. Plenty of agencies are available to assist you and provide advice if you are a victim of online fraud. The first place to start is your credit card company. If you are concerned that your card information has been stolen, call your credit card company and report it right away. In most cases, you will not be held responsible for fraudulent purchases on your account. You will also need to check your credit report, which you can do by visiting the websites of the three credit reporting agencies Experian, Equifax, and TransUnion and requesting your credit report. The law allows you to receive a free copy of your credit report every year. If you find any transactions that are fishy, follow the steps listed on the website to file a dispute.

You can also file a complaint with the Internet Crime Complaint Center (http://www.ic3.gov/default.aspx), part of the Federal Bureau of Investigation. Contact the Better Business Bureau (https://www.bbb.org/consumer-complaints/file-a-complaint/get-started) and file a complaint with them as well. If the business in question has a legitimate trust seal, contact the company that provided that seal and notify them of problem. If you discover that the business is fraudulently using the trust seal logo, you can still call the company associated with the trust seal as many of these companies want to be notified of fraudulent use of their logo.

Further Resources

We've collected a list of additional resources that can help you as you start shopping for your medication (and other products!) online. These resources will not only provide additional advice on securing your computer and browser, but will also teach you more about online safety and security, as well as medication safety.

Computer and Browser Security

If you'd like more information about securing your computer and browser, check out these resources:

• United States Computer Emergency Readiness Team — www.us-cert.gov (Check out the website's list of tips and advice for securing your computer.)
• Get Safe Online — www.getsafeonline.org (Tips, advice, and real stories about computer scams and other security issues.)
• Scambusters — www.scambusters.org (Many viruses and hoaxes are spread through email. Scambusters is an excellent resource for verifying the truth or falsehood of different claims that proliferate on the Internet.)
• PCMag — www.pcmag.com (An online magazine that discusses topics of interest to online consumers including security and safe online shopping.)

Online Shopping

These resources will help you learn to feel more comfortable about shopping online and provide additional advice about finding legitimate retailers:

• Safe Shopping created by the American Bar Association — www.safeshopping.org (A full listing of important information and topics for people who want to feel secure while shopping online.)
• Stay Safe Online created by the National Cyber Security Alliance — www.staysafeonline.org (A website dedicated to online safety and security, discussing topics such as safe online shopping, Internet security, and online safety tips.)

Online Pharmacies and Medication

The following resources will help you understand more about pharmacy responsibilities, your rights as a consumer, and medication safety:

Your state's Board of Pharmacy

National Patient Safety Foundation — www.npsf.org (Patient information to help you understand your rights as a patient and the responsibilities of pharmacies to make sure you get the right medication and are taking it correctly.)

Centers for Disease Control and Prevention, Medication Safety Program — www.cdc.gov/medicationsafety (A website run by the CDC with information about medications, side effects, proper drug disposal, and more.)

Safe Medication Use from Health Canada — www.safemedicationuse.ca (A site sponsored by Health Canada to inform patients about medication safety and how to report incidents and adverse effects.)

Quick Safety Tips

Print this page and keep it near your computer for quick tips and info when ordering your online medications.

How Do I Keep My Computer Free From Viruses?

Choose an online virus scanner and keep it updated. Best picks are:
- McAfee www.mcafee.com
- Kaspersky www.kaspersky.com
- Norton us.norton.com

How Do I Keep My Computer Secure From Hackers?

Keep firewalls turned on and clear your cache regularly using the recommended method for your operating system and browser.

How Do I Keep My Personal Information Secure Online?

Only send personal information over a secure webpage. Look in the address bar for "https" or a lock icon.

Only shop at sites that are verified by a third-party security company.

What Are the Signs of a Legitimate Online Pharmacy?

Only shop at online pharmacies with the following features:

Certified by CIPA

Require a valid prescription from your doctor

Have licensed pharmacists and physicians to answer questions and provide counseling

Sell safe, legal prescription medications and do not sell controlled substances

Have a full range of inventory, not just "lifestyle" drugs.

Promise to keep your personal information private and secure

Abide by the rules of HIPAA and PIPEDA

Do not send spam or other unsolicited marketing

Have a verifiable physical address and phone number

How Can I Verify an Online Pharmacy?

Before doing business with a pharmacy, always check on www.cipa.com to make sure that the site is truly certified by CIPA.

Check with other third-party ratings companies like PharmacyChecker and eDrugSearch to see both the ratings given by the site and the ratings provided by other consumers.

THE CANADIAN PHARMACY