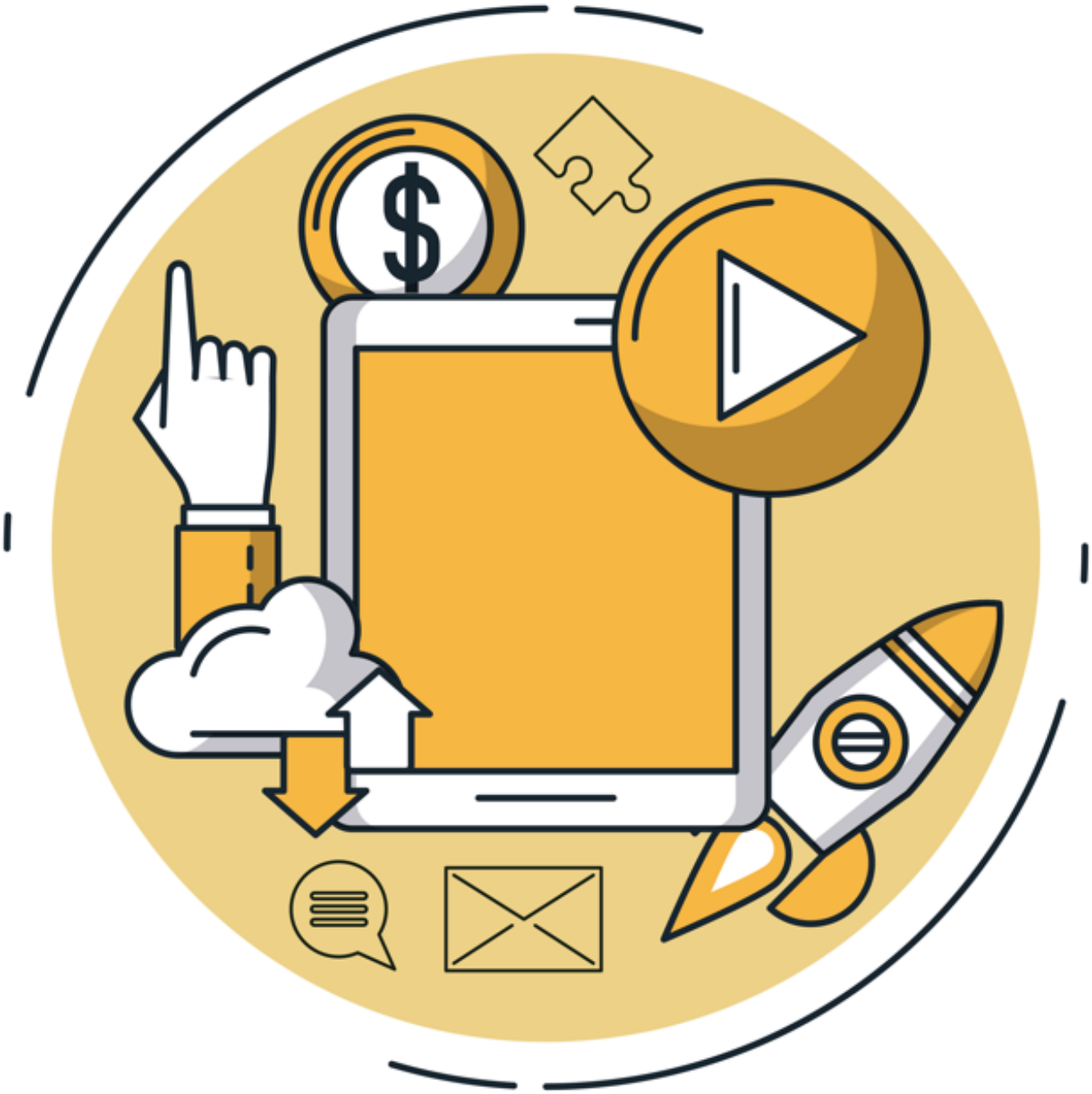
Do You Know You Can Get Scam Online?



ADUS MICHAEL

Do You Know You Can Get Scam Online?

Getting Scam Online is now simple and seamless because of visit on an online retail store you browse through its goods to get something for yourself or for the family.

But with simplicity comes bigger challenges. One of the top issues of online shopping is its security concerns. So far this year, over one thousand shoppers in Australia alone have already reported cases of scam online.

As the Internet becomes our everyday tool to trade and gossip and consume content, we can't stop buying and selling online, even though we are at risk of getting ripped off by get-rich-quick swindlers waiting to Scam Online users.

> *This eBook offers eight actionable tips for smart online shopping. These tips are categorized into two sections:*

Prevention tips—how not to get scammed while shopping online, and After the incident tips—what to do after you've been scammed. Let's look at each of these sections more closely. How to Avoid Online Shopping Scams. Start by answering these four questions:

Is the site secured?

The next time you visit an e-commerce store, the first security check if you don't want to be Scam Online, please do flick your eyes over to the address bar on the upper left side of the web page. Examine the URL of the page. Is it an HTTP or HTTPS?

Example HTTP and HTTPS sites from Safari

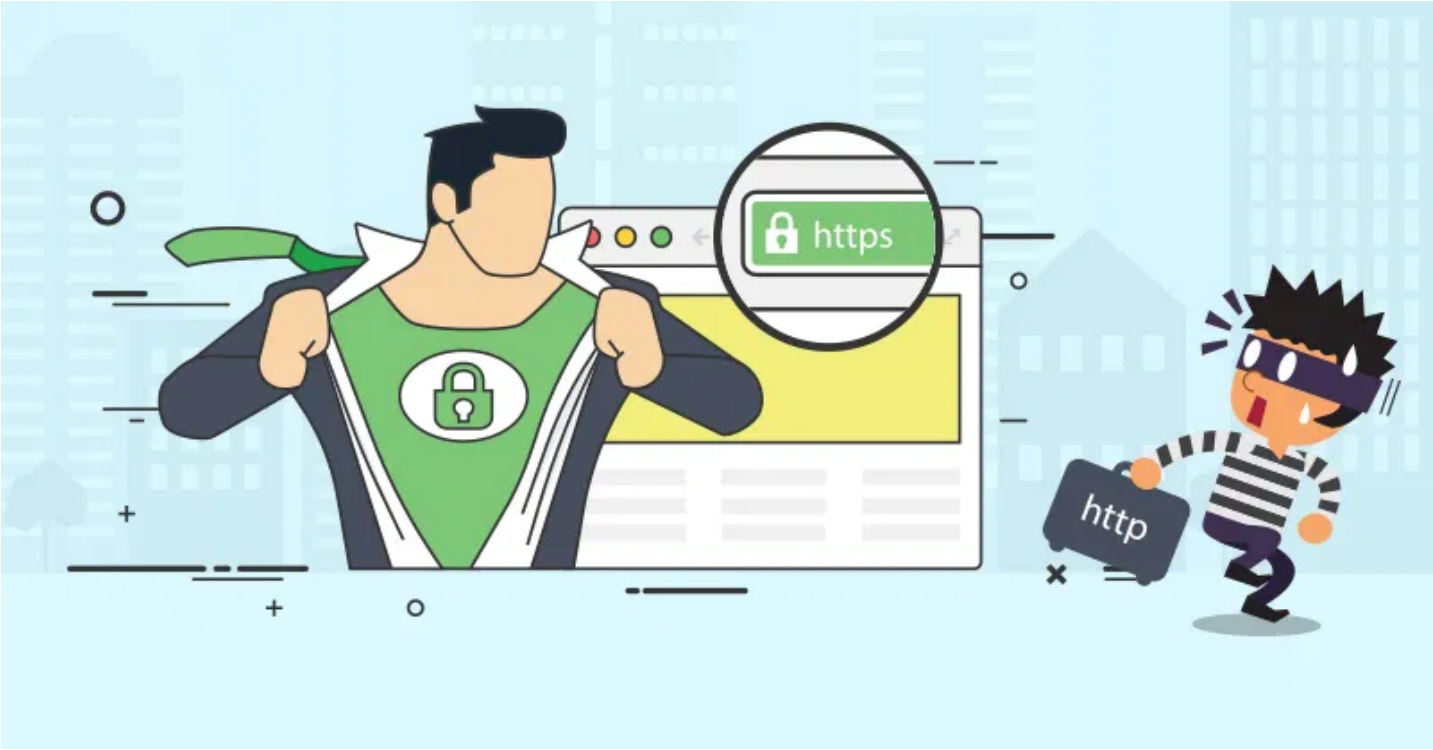
HTTPS means any information you enter into the site (e.g., username and password, financial or credit card details) will be encrypted and protected from interception or eavesdropping by malicious parties, Scam Online will be difficult.

Unfortunately, many phishing sites can appear safe simply because they use HTTPS. In this case, your information will still be encrypted, but it doesn't matter if you're submitting it to a phishing or scam online site that happens to use HTTPS. Your data is falling into the wrong hands regardless.

So in addition to checking for HTTPS, you should see if the company name is included in the URL. This can help you determine if the site is actually operated by the company and isn't an imposter or scam online site.

Not all sites use the type of technology that results in their verified identity information being displayed in the address bar and this isn't 100 percent foolproof regardless, so check your gut. If something seems "off," walk away.

Do You Know You Can Get Scam Online?



Is the site reliable?

You don't want to do business with unreliable websites—sites that house multitudes of hackers and cyber criminals or that sell bogus products and swindle users. You want to deal with reliable sites. But how can you tell if a site is reliable not a Scam Online site?

You review it. Before you buy anything from an online retail store, first run a background check on it. Or more realistically, Google it. See if other shoppers have used it, and critically review their feedback.

There are several review sites out there, but a great place to start is the Better Business Bureau. When conducting the review to avoid Scam Online, please pay attention to the answers to the following questions:

> *Do your peers buy from the site?*
>
> *What has their experience been so far?*
>
> *Is the experience good or bad?*

You, too, should focus on these key questions. They'll help protect you from being scammed as you shop on the Internet.

Is the offer too good to be true?

Fake e-commerce sites promote offers that are just too good to be true. They're not just giving out discounts. It's not a promo season. The site will put out an incredibly great sale that's just too good to be true, ready to Scam Online users.

For example, if you are shopping for a laptop computer that's within the range of $700 to $1000 and you come across an e-commerce store that boasts the low price of only $150, then that's a too-good-to-be-true offer. Steer clear of it. The people behind the site want to capitalize on the price to separate you from your hard-earned money.

Are contact details on the site real?

You might want to check the contact details of the site you are shopping on. As a rule of thumb, almost all businesses have their contact details—particularly their e-mail address, address, and phone number—on the "Contact" page on their site. You can use that information to confirm whether the retail store is genuine or fake.

How? Well, you don't want to drive miles away to confirm their office address, but you can easily look up their phone number in the reverse phone lookup directory to identify their location, ascertain the name of number owner, and compare the information you've found with what you see on their contact page.

If there is a match, that doesn't guarantee the site is real since the scammer might have copied the contact info from the real website, but if the information doesn't match, you immediately know not to trust the site, or at least do some more investigating. In this way, this strategy can be a quick way to rule out questionable sites.

Again, be sure to watch out for other signs of a scam site. Remember to look for red flags, such as bad grammar or misspelled words.

What to Do If You've Been Scammed.

As you can see from the previous section, it can be difficult to completely avoid the scam sites. No matter how vigilant you are, you may find yourself in a tough situation.

Do You Know You Can Get Scam Online?

> *Did you order something, but you haven't received the item you bought?*
>
> *Were you overcharged for an order?*
>
> *Are there additional charges on your invoice that you did not approve?*

In this section, we offer some actionable tips for what to do after you have been scammed online. Call your bank or Credit Card Company immediately.

If you have been erroneously charged, call your bank or credit card company immediately. Let them know what happened, so they can take the necessary actions to protect your future finances.

Your bank can put a hold on your account, your debit card, and any checks. Your credit card company can freeze your card. Many finance companies also offer fraud protection, which covers certain charges made without your consent, but you have to report the errors promptly.

File a complaint (if you bought from a marketplace).

Next, file a complaint if you made the purchase in a marketplace, such as eBay or Amazon. Most of the online marketplaces are reputable, so they'll help you to investigate the culprit and retrieve your stolen money or receive the product accordingly.

Even freelancing sites have policies in place to protect their users from fraud. For example, a friend who offered a service to a client on Fiverr notified the company after the client refused to pay for the services rendered.

After Fiverr investigated the claim, the company immediately deleted the fake client's account. The contractor didn't get his money, but at least justice was served.

Get your money back.

Some online shoppers completely lose hope, thinking that they'll never get their money back after they have been scammed. While it is difficult to get your money returned to you after you've been ripped off online, there are some chances to get your money back.

For example, if you ordered a product from an e-commerce retail store using your PayPal account and your order hasn't been delivered, PayPal Buyer Protection can cover you.

However, there are limits to what they can do. If a scammer set up a convincing clone of the PayPal payment form that just extracted your bank details, you will not enjoy the PayPal Buyer Protection. Keep this in mind anytime you're shopping online.

One more thing to remember is a benefit of using credit cards versus debit cards. As mentioned earlier, both banks and credit card companies have certain protections in place against fraud.

However, if the fraud occurred in your bank account, it's likely the funds will be withdrawn from your account when the order goes through and you will have to wait to be reimbursed.

A credit card can act a little like a buffer – an extra step between the fraudulent charge and you actually having to pay – and many cards offer some type of purchase protection for situations like this.

File a police report.

Above all of these, you should also consider filing a police report if you have been scammed while shopping online. You need to file a police report for several reasons:

You're increasing your chances of getting your money back. Involving security personnel in the search to uncover the thief who stole your money, assuming the money was stolen from your bank account, is good for you. You've just been robbed online.

Do You Know You Can Get Scam Online?

Reporting the case to the authorities will intensify the search for the culprits, which will increase your chances of getting your stolen money back.

Your bank or credit card company will likely need a copy of the police report.In some instances, your bank and/or credit card agency will request a copy of the police report you've filed.

So don't wait. Call your local police immediately with the non-emergency number, not 9-1-1, and report the case to the computer-related crimes division.

It’s about taking decisive action.

Conclusion

It’s exciting to order stuff online as you recline comfortably on your couch, but the experience can be devastating when a fake seller steals your money.

You can help avoid getting scammed by performing the basic checks mentioned above, like looking for HTTPS and other identifying information about the vendor or checking reviews other buyers’ reviews.

As mentioned throughout this piece though, none of these actions is foolproof, so if you find yourself a victim of online shopping fraud, take immediate action by calling your bank/credit card company immediately and filing a police report.

With these tips, you can stress less as you shop online, but remember there is no way to stay 100 percent safe from Scam Online. Fortunately, the more careful you are, the more likely you will be to spot and avoid these scams.