

How to avoid getting scammed on the Internet

This chapter is all about protecting yourself when you do business or make purchases over the Internet. Over the years I've heard a lot of horror stories about people getting ripped off by unscrupulous places and this guide will give you the information to make sure it never happens to you. There are some very important things to remember and some warning signs to watch for when dealing with any company or person on the Internet.

Most Important, always use a credit card when buying something on the Internet. Never use a check card (those ATM cards with a Visa or MasterCard logo on them). With a real credit card you have chargeback protection in the case of fraud. Visa/MC allows up to six months from the date of purchase but it's very important to remember that your issuing bank controls the actual amount of time, call them to find out. Most allow 60 days at the minimum and others allow the full six months (but it's rare to be sure to call so you know how much time you have). A real American Express card (one issued by them and not a third party like a Delta Sky miles card) allows seven months of protection and I hear from a friend his Platinum Amex card allows 12 months.

If you use a check card that draws from your bank account there is no way to chargeback if you order something and they don't deliver or have some other problem. Some check cards only allow you to recover funds if it's reported within a few days and that's never enough time to avoid a problem if you have one. The same with online checks, wire transfers, etc. Always use a real credit card when dealing with a company you don't know.

If for example some company doesn't deliver a product you ordered, you can contact your credit card company to initiate a chargeback. Some issuing banks require a signed affidavit, others can do it over the phone and often ask you FAX them details, receipts, contracts, etc. with a letter describing your dispute. They decide whether they can just charge it back and that's the end of it, or if they have to forward the dispute to the merchants processor.

If they do then the merchant has 10 days to respond with a rebuttal, or if they don't respond you win it automatically. They typically ask the merchant for a tracking number and proof of delivery if you never got the item. In cases of Visa/MC if they dispute it, you get a chance to dispute their rebuttal and it goes to Visa or MC for mediation and they make the decision from there. This is a powerful tool for the consumer in cases of fraud or non-delivery of an item you purchased. The rule is, if a place doesn't accept credit cards it should be a red light. Anyone can get a Paypal or 2checkout account these days so there's no excuse not to accept them. Also if they send you a form to sign and FAX back to them and it says anything like "waive the right to chargeback" then forget it, you've found yourself a scammer.

I would strongly recommend that if you can qualify, get a real American Express card for business or online purchases. I like the Amex Blue card since it has no annual fee, a low APR, and you can pay over time. With the seven months of chargeback protection you can't beat it. I've heard the Platinum Amex has 12 months, but it can be very difficult to qualify for and the annual fee is something like \$400.

Other payment methods

If a place insists you send a check or payment via a prepaid FedEx, UPS, Airborne, or other commercial carrier then don't do business with them. Professional swindlers often refuse to accept US Mail since it subjects them to very harsh mail fraud laws and Postal Inspectors who have very broad powers to prosecute them. Especially true of investment schemes, they will try to pressure you into sending a check or money order via a private carrier and will make excuses not to accept US Mail.

Others will try to get you to do a wire transfer, sometimes offering the excuse they will take the 3% credit card fee off a large purchase. It's against the rules of anyone with a merchant account to offer a discount or add the 3% fee to someone using a credit card. The merchant always has to pay that fee, not the customer. I emphasize this as we've heard of many people who bought into some program

and were urged to overnight a check (many times they will offer to overnight a prepaid envelope to you to return to them via a private carrier. If you hear that kind of talk from anyplace, run far and run fast.

Check their web site for contact information

I think we've all seen these, places that don't list their company name, address, phone number, or even email address. If a place only has a web site form to contact them with no other information, I would pass on them. If you can't get in touch with them when you're looking to buy or get more information then it's very likely they aren't a legitimate business. If they are on a free web hosting company like tripod.com etc. then that's even worse. Professional Con-men try to hide their tracks, I've seen many overseas based software pirates and scammers with sites like that and it's a dead giveaway if they don't have contact information.

If they use a PO Box with the Post Office (not a private place) then there is a way to get their real address. You can get the actual address on file with the post office for anyone who does business with the public. Just call the local post office where the box is and ask them for the registered address they used for that box and they will give it to you. That address is verified by the post office when they apply for the PO Box. They mail them a form which must be returned to verify that their mailing address is valid. The same is true for the private mailbox places but they are not required except for a subpoena to reveal the actual address of their customer.

Beware of typed testimonials

This is something you should be especially aware of. Those testimonials you see typed up on web sites are very easy to fake and usually impossible to verify since most people don't want their personal contact information on someone's web site. I wouldn't want 10-20 people a day emailing me or calling me to verify or ask questions about a place I did business with, even if I liked their product enough to write a testimonial letter. Check to see if all the letters are written in the same style, or if they are "over the top" with praise. If it sounds more like sales hype than what a regular person would write then I'd be cautious. Even with legitimate companies they usually won't allow you to call people who wrote the testimonial due to a privacy policy or just not wanting to bug a good customer constantly with people who want to verify them. It's a mixed bag so you really have to use your judgment to decide if the letters are authentic.

Overseas Companies

Doing business overseas is simply much riskier than in your home country. This is because your legal recourse is much more limited in case they do not deliver or some other problem. Again, using your credit card will give you good protection. This will really vary depending on what type of business you're doing. If you pay someone to purchase software or maybe have them design a web site there's not much risk for a credit card purchase. Of course if you're paying a firm to write a program for you exclusively, then they decide to start selling the program themselves it can be very difficult to go into litigation depending on the country they reside in. It might also be more expensive than it's worth in some cases depending on the transaction.

If you use an escrow service, make sure they are well established.

One of the more recent scams is places who sell via EBay or maybe from a professional looking web site and offer an escrow service for large ticket items. The problem is that "escrow service" is just a front company for the place who sold you the item. They will not deliver the item, and keep the funds. It's VERY important to verify any escrow service with a lot of research to find out if they are indeed legitimate.

Never respond to any email requests for information, known as "phishing"

Your bank, Paypal, EBay or any company is never going to send you an email because they lost your personal and banking information. Other times you'll get an official looking email (many times with a valid return address to that company and graphics ripped off from their web site to make it look authentic) that says your account will be suspended if you don't click the link and verify or re-enter your information. What happens is you're redirected to a web site (usually an IP address in China) that looks legitimate and it will have a form to enter your username, password, bank and credit card details, the whole nine yards. The problem is you just gave all that information to a hacker who's going to use your credit card, empty your Paypal account, and so on. Never ever respond to an email like this, your bank is not going to lose all your personal information but magically retain your email address.

This may sound simple but you wouldn't believe how many people fall for this each year. The emails look authentic and many people just click them not even thinking about it.

If they don't have a refund policy don't do business with them

Another obvious one but it's important to look for on a web site. If they don't have a policy posted don't assume they have one. The most important point to this is that's a sign they don't stand behind their products. If they offer a seven day refund policy on something that's going to take you three weeks to read then something is up. Don't buy from companies that give you the bums rush when it comes to a refund policy. Of course there's some merchants like those who sell CD's or software, it's common practice not to accept returns after someone opens MS Office and installs it or buys a DVD movie and breaks the seal. Sometimes they will put "all sales final" or some other disclaimer and that should get you worried as it could be to assist them in disputing a chargeback if they ship shoddy merchandise.

Make sure they have an SSL Certificate when filling out a credit card order form

If a merchant is using a third party processor like Paypal then you don't have to worry, but if they have their own merchant account and order form you must check on this. Simply look in the lower right side of your browser to see if the padlock icon is closed or open, if it's closed you're on a secure page. If it's open then don't enter any information you wouldn't mind having on the Internet. When entering information on a secure page the connection between your browser and their server is encrypted so your information can't be intercepted by any of the machines between you and them. Whenever you do anything on the Net, you pass through dozens of other systems and any of them can setup a packet sniffer to grab 15 or 16 digit numbers (Amex cards are 15 digits, Visa/MC are always 16 digits) passing through. They don't even need your expiration date because when a card is run, the merchants bank just checks to see if the card is expired or not, they don't check to see if the expiration date is correct or not.

If you have the option, use a third party processor like 2checkout.com or Paypal

The reason for this is simple. When you use a third party processor to pay for an item versus placing it direct with the merchant, the place you're buying from never sees your credit card information. Most small businesses don't have security anywhere near a place like 2checkout.com or Paypal. The big processors are fortresses as far as security compared to a standard web site that's on a hosting company somewhere. Worse yet, many people with merchant accounts have a form that mails them the order you placed, including your credit card information so they can run it on a terminal or software at their home or office. This gives a lot more exposure and chance to be intercepted as it's emailed to their ISP, then again when they retrieve it from the server to get their email with your order. No place is invulnerable to hacking, but the big processors have full time security people to keep them secure and your information is a lot safer stored with them.

In Summary

The Internet is really much more like real life than we realize. Just as in real life there's good and bad people on the Internet. Using this advice to protect yourself and doing some research on that company you're about to do business with will pay big dividends in your peace of mind and success. We at Crown Industries wish you the best in starting or running your Internet business, and hope you avoid all the pitfalls when it comes to purchasing goods and services on the Internet.