Online Shopping Safety

Risks and Recommendations

Information and Advice from Zeezaw

April 2010

Release 1.0

Overview of Internet Shopping

The first Internet stores opened in 1996 and since then, the number of online retailers has grown rapidly. At present it is estimated that more than 600,000 people are employed either directly or indirectly in the UK's estimated 150,000 online retailers.

Internet retail has become huge business and in recent years has been seen to rival traditional bricks and mortar stores for profitability. In many cases, online retailers have surpassed high street stores in terms of low prices, selection of goods and convenience.

It has taken some time for confidence to grow in the use of online stores largely to the novelty of the technology and the perceived risks involved. Although the risks involved are not as great as they were in the past, largely due to secure payment choices and an awareness of the threats posed, the risks still exist.

The following section covers the most common risks after which, we discuss some suggestions about how to reduce the chances of being caught out.

Risks

Buying counterfeit, damaged or stolen goods

Whether intentionally or not, the risk of receiving counterfeit, damaged or stolen goods exists when shopping on the Internet. This is detrimental to the consumer in many ways, the most obvious of which is being landed with a substandard product. However, it is also possible for the customer to put their own health at risk by purchasing an item which is simply dangerous eg. containing faulty electrical components, ingredients that are not safe for human consumption, toxic additives in paints and inks, etc.

The dangers of purchasing pharmaceuticals online cannot be understated. There has been a growing trend in recent years of counterfeiting drugs and health products to capitalise on the growth of online pharmacies. Counterfeit drugs can cause damage either by containing harmful ingredients or by simply not containing any active ingredients at all, leading individuals to believe they are being treated when they aren't.

Delay and hassle with online purchases

Sometimes a company can take a long time to respond to an order placed online and to deliver what has been ordered.

To avoid the stress of delays or hassles with a vendor, we would recommend that you use a search engine such as Google to see if anyone else has had problems with the vendor before you go ahead and make a purchase.

Unfortunately sometimes mistakes are made, stock is not available, numbers of orders is underestimated, etc. so you should not immediately disregard an online store due to delivery or delays in other customer's purchase. Dell, for instance, have had several issues with delayed deliveries yet is still a reputable and trustworthy company.

Paying for goods that never arrive

This can happen quite frequently, but fortunately as consumers we have considerable protection from this when using reputable vendors. Sites such as Amazon or eBay offer ways to compensate consumers who could be ripped off by fraudulent third party sellers. Again we recommend you carefully check customer reviews and rating before making your purchase.

Many online retailers do not offer any protection against missing or undelivered goods, however, depending upon where you live there should be a trading standards organisation that can help. For example, in the UK there is the Trading Standards Institute (http://www.tradingstandards.gov.uk/) that provides advice on what steps you can take.

Misuse or theft of credit card or banking details

There are a few ways in which criminals try to obtain your credit card or banking details:

Phishing

This is popular because it is incredibly easy to do. An e-mail is written that pretends to be from a bank or other financial organisation, claiming that you need to log in to their website to confirm or correct your personal details. The links on the e-mail will be faked to direct you to a website that looks very much like the real one. These e-mails get sent to millions of people, so only a very small number of responses will make it worth while for the criminals to continue. They cast their net wide in the hopes of catching a few victims, hence "phishing". The change of the "f" to "ph" in the word is simply a thing that hackers have done for years.

Clues to watch for:

- Is the spelling and grammar correct throughout the e-mail?
- Are you addressed by your full name or does it say "Dear customer"? Another ploy used here is to take the start of your e-mail address to try to fake a greeting, eg. if your e-mail address is simon@somewhere.com, you may get "Dear simon".
- Does the e-mail contain all the correct graphics for the company?
- Hover your cursor over the links and check the status bar at the bottom of the screen to see where the link is going to take you. The text that is displayed is not necessarily the same as the actual link!

- Is the e-mail suggesting that you are required to provide some personal/financial information? Reputable companies, especially financial organisations, will never ask you for this by e-mail.

If all of the above are answered to your satisfaction, then perhaps the e-mail is authentic and the company really does want you to visit their website. If so, you can go to their site by typing in the address or by searching for them on Google, thus avoiding the link in the e-mail.

This link will take you to the fantastic Anti-Phishing Work Group (http://www.anti-phishing.com) who offer advice on how to check the site you are visiting is legitimate.

Hacked email accounts are frequently being used to send spam containing details of discount electrical, pharmaceutical, watches and designer clothing stores or pretending to be a friend recommending items like this. This may at first appear to be an e-mail from someone that you know, but the way the e-mail is written will usually give the game away. These vendors are to be avoided at all costs! You would almost certainly be ripped off paying for goods that never arrive, receive stolen or counterfeit products, or have your credit card details stolen and passed into the hands of criminals.

Trojans

Like the Greeks hidden in the famous wooden horse, e-mail attachments can contain programs that can run on your computer. These are harmless unless you open them. There are a few ways in which the criminals will encourage you to open them. One of the most common ways being faking the name of the attachment so that it looks like an innocent file, eg. a graphical image or a document. Many of these e-mails also contain text that urge you to open the attachment by promising a variety of potential benefits.

To avoid problems with Trojans (and a few other types of virus), never open attachments on an e-mail unless you know what it is and why it was sent.

Man-in-the-middle

This involves intercepting your communications, very similar to the concept of “tapping” a telephone. As your data flows between your computer and the website you are viewing, a third-party can get to see what is being transferred. In order to do this, the criminal needs to find a point in the communication link at which they can listen in.

In this case, the percent intercepting the information may or may not change the information being passed to and fro.

This is much more technically sophisticated than phishing, but website owners can avoid it very easily by simply adding encryption to their site. The encryption process (normally using the “https” protocol for websites) adds checking to make sure that only the computers at the ends of the link can see what is going on.

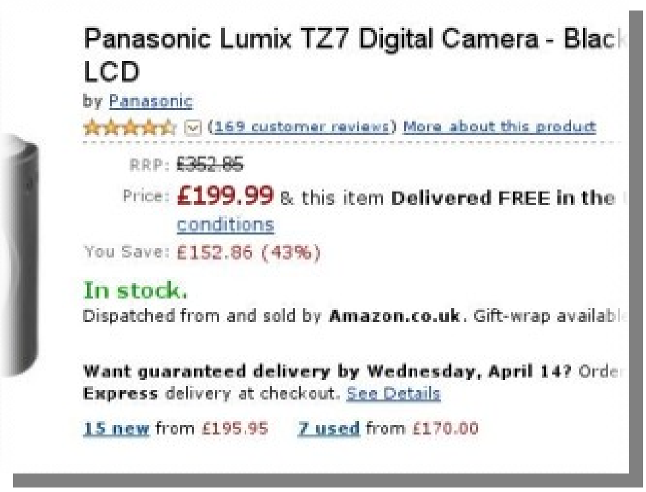
Emotional distress linked to the above

Unfortunately there is no easy way to cope with the stress of knowing you have been ripped off. It happens to a great number of people every day and it is a sad fact that fraudsters are using every more sophisticated techniques to get to our cash. But by remaining vigilant and doing a reasonable amount of research before you buy and following the above advice you can put your mind at rest that you are remaining as safe as possible.

Recommendations

Where possible, use trusted websites/vendors

There are many simple ways to improve your safety when buying online. By shopping from trusted vendors you can be sure to stay safe. Sites like Amazon and Play are respectable outlets and buying from them is a safe, tried and trusted experience. Bear in mind that both sites offer goods from third party sellers. The screenshots below show how this information is presented:



Panasonic Lumix TZ7 Digital Camera - Blac
LCD

by Panasonic

★★★★☆ (169 customer reviews) More about this product

RRP: ~~£352.85~~

Price: £199.99 & this item Delivered FREE in the
conditions

You Save: £152.86 (43%)

In stock.

Dispatched from and sold by Amazon.co.uk. Gift-wrap availabl

Want guaranteed delivery by Wednesday, April 14? Orde
Express delivery at checkout. See Details

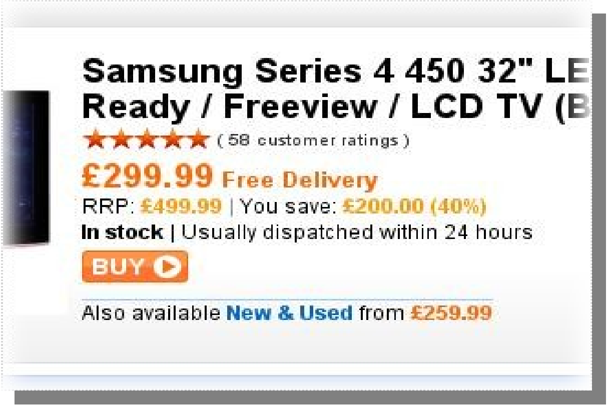
15 new from £195.95   7 used from £170.00

Screenshot from amazon.co.uk

This screenshot, taken from the Amazon web site shows that this particular product is available from three sources. Firstly, it is available direct from Amazon itself for £199.99, indicated by the “Dispatched from and sold by Amazon.co.uk” text. Second, there are 15 third-parties selling the item, where the cheapest option is £195.95. Finally, there are 7 other third-parties selling the item starting at £170.00.

Note that third-party sellers may not offer the same kinds of guarantees and delivery options as Amazon. However, if you click on the “15 new” or “7 used” links, this shows the sellers information, including information about feedback that they have received from previous sales. In general, it is reasonable to assume that a seller with a large amount of positive feedback is likely to be a safe option.

This next screenshot shows a similar selection of options on the Play.com website. In this case, clicking on the “New & Used” link shows a list of all third-parties selling the item. Like Amazon, they have a feedback system to help customers judge the trading history of the sellers.



Samsung Series 4 450 32" LE
Ready / Freeview / LCD TV (B

★★★★★ (58 customer ratings)

£299.99 Free Delivery

RRP: £499.99 | You save: £200.00 (40%)

In stock | Usually dispatched within 24 hours

Also available New & Used from £259.99

Screenshot from play.com

Many websites that allow third-party sales have feedback systems like this and it is usually worth a few minutes for a quick background check before making a purchase.

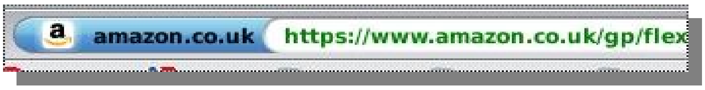
Check your personal/financial information being handled securely

When you are going to provide personal or financial details on a website, you should ensure that your details won't be leaked as they travel between your computer and the website that you are using. Your web browser takes care of this using an extra level of security called SSL[1]. This uses a security certificate provided by the website to encrypt all the information that goes to and fro whilst you are connected. There are several ways that your browser will indicate that this is working:

1. The URL (website address in the address bar) will start with **`https`** instead of just **`http`**
2. There should be a padlock symbol somewhere on the browser. Please note, a padlock icon displayed on the website itself is *not* an indicator of security.
3. On some web browsers, further indications are used, such as the address bar being highlighted.

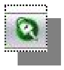
Examples:

Firefox 3.6:

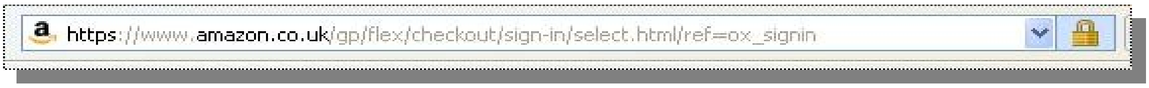


amazon.co.uk https://www.amazon.co.uk/gp/flex

On the status bar at the bottom of the screen is:



Internet Explorer 8.0:



https://www.amazon.co.uk/gp/flex/checkout/sign-in/select.html/ref=ox_signin

The key thing to note at this stage is that SSL is just a single piece in the security jigsaw. All it does is to ensure that your communication isn't being intercepted and filtered off to somewhere else as it travels across the internet. It *doesn't* guarantee anything about the trustworthiness of the company/individuals that are operating the website that you are viewing.

Make use of vendor review information where available

As well as the “star rating” or “percentage quality” feedback, most of these systems allow written feedback or reviews as well. Look out for previous issues such as non-deliveries or faulty goods. Sometimes bad feedback is left for malicious reasons, not because of truly bad service. Watch for responses by the seller to see what their

[1] SSL – Secure Sockets Layer

attitude is and how they deal with such feedback.

Use search engines (eg. Google) to find more information

If you are planning to make a purchase through a site you don’t recognise then be sure to be wary of any goods that seem very cheap, or too-good-to-be-true. This doesn’t guarantee that the deal is rotten but be careful and try searching for any news and information about the website and/or seller. If customers have previously been duped then it is quite likely that you will find a forum or blog warning others about the suspect service!

Keep copies of all correspondence

When you place an order online, most companies will send you an e-mail confirming the order has been received. Some will follow this with further order processing information and dispatch notifications. Keep all of these e-mails. If anything goes wrong during or after the order, you will have all the information you need to explain what happened, including timestamps to accurately demonstrate when things happened.

Sometimes you need to fill in an online form to complete information or file a support request/complaint. In this case, you should ensure that you copy the message you send (before you click the send/submit/next button) and save a copy on your computer with a note of the date and time. This is because you don't always get a copy of messages sent this way and that could mean a break in your record of communications.

Take even more care with health products

Be wary of any site promising a “miracle cure” as sadly most of these products simply do not work or, in the worst case, can actually be harmful. We strongly recommend avoiding online pharmacies other than known, reputable brands. In the UK, for example, there are Boots and Lloyds Pharmacy. Again, buying prescription drugs online can be incredibly dangerous and there have been reports of fatalities caused by harmful counterfeit drugs. We would recommend that you ***never*** buy prescription drugs online.

For some case studies highlighting the hazards of this, see:

China's deadly trade in fake drugs (Channel 4 News):
http://www.channel4.com/news/articles/society/health/chinas+deadly+trade+in+fake+drugs/595147

Fake drugs trade on the rise: EU (The Independent):

http://www.independent.co.uk/life-style/health-and-families/health-news/fake-drugs-trade-on-the-rise-eu-1835977.html