**Shopping online? Eight ways to beat scams today**

If you love shopping online, you’re in great company. Global [revenues from retail e-commerce are set to more than double to $4.48 trillion between 2016 and 2021](https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/). The growth of digital marketplaces means consumers can increasingly find what they want, when they want it more easily than ever before. But online shopping comes with risks too. Luckily, there are a few simple steps you can take to reduce your risk of falling victim to online shopping scams.

**Spot fake sites**

Online shopping means you can beat the crowds to get the products you love from anywhere in the world. But scammers know you trust familiar brands, so they often use branding you know to catch you out. Check the domain name – if it sounds like a brand you know but isn’t the official website, that could be a warning sign. There are other red flags too - legitimate sellers will rarely use domain names ending in .net or .org or make mistakes with spelling and grammar.

But you could still be caught out - some scammers use convincing layouts and stolen web addresses. If you’re not sure, look at the real brand website – it should display scam warnings for you to check. Always look for web addresses that begin https:// and show a green padlock sign. This means information travelling between your computer and the website will be encrypted and scammers won’t be able to steal your payment details.

**Trust the website, trust the shop?**

Platforms like Amazon, Alibaba, eBay and even Facebook enable small sellers to connect with consumers all over the world. But just because you know the platform, that doesn’t mean you can trust every seller on it. Use a secure payment system if there is one and never pay by wire or bank transfer. That way, the seller can’t steal your payment details and if anything goes wrong you have a chance of getting a refund.

**Think like a scammer**

When you shop online, you share personal data like your name, address and bank details with the online seller so they can process your payment and deliver your order quickly and easily.

But fake sellers can use details like your name and address to steal your identity. If you don’t use a secure payment system, they can steal your card details and use them to make other purchases. If you give them passwords you use elsewhere, they could even access your other accounts. [Half a billion digital personal records were stolen in 2015](https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/) - take care only to share this information with sellers you trust.

**Don’t trust every deal**

Everyone loves a great deal – but if you suspect it’s too good to be true, you could be right. Fake sellers know they can entice you with offers to push you to make a decision before you’re really ready to buy. No matter how exciting the offer, make sure you trust the seller before you buy.

**Get to know your seller**

Reputable sellers will make it easy for you to find out who they are. Check the contact details of the seller. Can you tell who they are and how to get in touch with them? Be wary of sellers that only give a mobile number – that makes it harder to trace where they really are. You should also be able to find a returns and cancellation policy, terms and conditions and a privacy policy explaining what they will do with the information you share with them. You may want to meet up with the seller in person to inspect an expensive product before you buy or to pay in cash. If you do this, stay safe – always meet in a public place, tell your family where you are going and take your phone.

**Wise up to fake reviews**

You can check up on a seller by looking at reviews of their products across a range of different websites. You’ll want to see a range of different reviews from accounts that have reviewed lots of products over a long period of time. They should describe the specific features of the product and sound like they were written by different people – if several reviews sound very similar, they could be fakes.

**Know the best ways to pay**

Taking these steps can help you avoid online scams – but sophisticated scammers could still catch you out. That’s why it’s important to make sure you have a chance of getting your money back if you need to.

If a seller insists on payment by an unusual method such as a pre-loaded money card, bank transfer or wire service, they’re likely to be a scammer. Never agree to this – if anything goes wrong, your money is unlikely to reappear. If you pay by credit or debit card or via a secure payment system like PayPal or Alipay, you may be able to speak to your bank and reverse the transaction.

**Report the scam**

If you suspect a scam, contact the seller first - they may have a good explanation for the problem. But be wary if they ask for personal data from you – they could still be trying to steal your information. If they do turn out to be a scammer, you can still act to stop them tricking other people the same way. Many governments run websites where you can see scam alerts, [report scams](https://www.icpen.org/avoiding-scams) to the police and access help and support. The International Consumer Protection and Enforcement Network (ICPEN) also runs [Econsumer](https://www.econsumer.gov/#crnt), a site where you can report international scams help consumer protection agencies to spot trends and tackle scams worldwide.