Let's make it a safe and happy experience

Christmas is almost here again, and more of us than ever will be buying for friends and loved ones (and maybe ourselves) on the internet.

Shopping online offers great convenience plus the widest range of goods, the best choice of places to buy them and the chance to find and compare some great bargains. But Christmas is also a favourite time of year for fraudsters, who take advantage of the millions of people doing their shopping on the internet.

Get Safe Online has joined forces with Barclays, Kaspersky Lab (the internet security people) and the City of London Police to give you some handy tips about keeping safe online while you're doing your Christmas shopping this year.

BARCLAYS

CITY OF LONDON POLICE

KASPERSKY lab

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

Helping you to have a very merry festive season and happy New Year!

What is Get Safe Online?

Get Safe Online is the UK's leading source of unbiased, authoritative and easy-to-understand information on protection against fraud, identity theft, viruses and many other problems encountered online – as well as physical computer theft/loss, backups and related topics.

Aimed at consumers and small businesses and jointly funded between the Government and Private Sector, Get Safe Online is the Government's default online security advice channel. A world-leading initiative, Get Safe Online is a not-for-profit organisation.

BARCLAYS

CITY OF LONDON POLICE

KASPERSKY lab

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

GET SAFE ONLINE .org

www.getsafeonline.org

OFFICIAL PARTNERS

HM Government | Cabinet Office | Home Office | Department for Business Innovation & Skills | NCA National Crime Agency

ActionFraud Report Fraud & Internet Crime actionfraud.police.uk | National Fraud Intelligence Bureau | Association of Chief Police Officers | Bob's Business

Microsoft | Ofcom | BARCLAYS | creativevirtual

Norton SECURED powered by VeriSign | HSBC | KASPERSKY lab | Gumtree | PayPal

Christmas Shopping online...

BARCLAYS

CITY OF LONDON POLICE

KASPERSKY lab

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

GET SAFE ONLINE .org

Your top Christmas shopping tips…

SECURE WEBSITE?
Before you even think about entering your debit or credit card details, make sure the payment page is secure by checking that the address starts with 'https' (the 's' stands for 'secure') and there's a padlock or unbroken key symbol in the browser window. Make sure your home WiFi is secure too.

AUCTION SITES
Auction sites such as eBay are a popular way of buying presents. Remember to always use insured methods of payment for the site rather than making direct payments to a seller, and if you're going to pick up your purchases in person, take someone with you or let someone know where you are going.

TOO GOOD TO BE TRUE?
There's a saying: "If it seems too good to be true, it probably is". This is especially true of the internet, so if you find or are emailed about a bargain that seems just too cheap, it could well be a scam, the item is a fake, it doesn't match the description or it simply doesn't exist. If the seller doesn't check out … check out of the website!

DON'T TRANSFER MONEY
An authentic seller will ask you to pay by card on a secure payment page, or occasionally by cheque. However tempted you are because it's the "last one in stock" or "two days before Christmas", never transfer money into the seller's account … you may never see the goods or your money ever again.

FINISHED YOUR PURCHASE? ALWAYS LOG OUT
When you've finished your online shopping session on a website, always log out of the site … it only takes a second. Sometimes, just closing the window doesn't mean you've logged out, and someone else could gain access to your account and personal details. Don't forget to save the confirmation email as a record of your purchase.

EMAIL LINKS AND ATTACHMENTS
We've all received emails urging us to click on a link to reveal a special offer, or open an attachment containing some great news, or to "confirm details". Sometimes these are from reputable online stores and banks, but often they're scams and could lead you to reveal your personal details or download malware. If in doubt, delete the email and don't pass it on.

CHECK YOUR STATEMENTS
During this busy shopping time, it's a good idea to check your statements regularly online to keep track of what's going out of your account. Contact your bank straight away if you see any unfamiliar transactions. Make sure your bank has your up-to-date contact details too, so they can contact you quickly if they spot anything unusual.

NEW SMARTPHONE OR TABLET?
Remember to protect phones and tablets with internet security software. Also, if you're buying one for a child or young person, get some parental control software loaded before you give it to them and chat about how to use the internet safely.

SCAM PHONE CALLS
Beware of fraudsters posing as retailers calling to confirm an online purchase. When you can't recall it, they'll suggest your card has been compromised and that you call your bank immediately. But they stay on the line, pretend to be your bank and trick you into revealing your financial details. Use a different phone line to call your bank, or call someone you know and trust first to make sure your line is properly disconnected. And never disclose your card details or other security or account information to a caller.

SOCIAL NETWORKING SPECIALS
Social networking sites are increasingly used by fraudsters to spread their scams too. So again, if you see a post promising a free giveaway or cut-price offer that seems too good to be true, think twice before you follow it.

You'll find all the free, impartial, easy-to-understand advice you need on staying safe online at **www.getsafeonline.org**

If you think you have been a victim of fraud, report it to Action Fraud by calling **0300 123 20 40** or by visiting **www.actionfraud.police.uk**

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk