More of us these days are shopping online, buying everything from electronic devices, white goods to clothing.

Unfortunately, in our haste to grab a bargain, many of us can fall prey to internet fraudsters.

To help protect online shoppers from being deceived and duped out of their money, the Fraud Investigation Team at Greater Manchester Police has issued a number of points to think about before buying online.

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

GREATER MANCHESTER
POLICE

1 VALUE THE WEBSITE OVER THE DEAL

It's not unusual for a number of shopping websites to suddenly appear online during certain of times of the year, such as the summer holidays or the run-up to Christmas.

Some of these websites can be fronts for cybercriminals who are simply after your personal and financial information. Shop with websites that you have used before and trust. Even if the prices aren't the lowest, it may cost you less in the long run.

Also, always check that the website has a physical address and a working contact telephone number.

2 BE WARY OF EMAILS PROMISING GREAT DEALS

Phishing emails can offer goods at bargain prices. These emails often contain links to sites that can mimic a genuine retailer's website. Customers, having been deceived, can unknowingly pass on their financial details to cybercriminals.

Check the email address of the sender - if it doesn't look genuine delete it or send it to your junk folder. Always type in the retailer's web address or search for them using a search engine.

3 IS THE WEBSITE SAFE?

Before entering in your payment details on a webpage, make sure it's secure. The web address of the payment page, where you enter your payment/card details, should begin 'https://…'. The 's' stands for secure.

Also, look out for a small padlock symbol in the right of the address bar - this means any data sent is encrypted, making it harder for cybercriminals to steal your financial information.

4 ARE YOU UP TO DATE?

Always make sure that the device and software you're using to shop online is kept up to date. Cybercriminals can take advantage of equipment and software that hasn't been updated, making it easier to steal your personal and financial information. When prompted, take the time to download the latest software updates.

5 PAY THE RIGHT WAY

When making a payment to a company website or private seller, always use a secure method such as PayPal, where money is transferred between two electronic accounts. If you do not have a PayPal account and you're buying something valued at £100+ always use a credit card, you'll have more protection if something goes wrong compared to using a debit card.

Never transfer money directly from your account to someone else's. If you do, know that you have no protection from losing that money.

6 NEVER BUY USING PUBLIC WI-FI

Free public Wi-Fi can provide a convenient internet connection, but be aware that they are a target for cybercriminals. Never shop online, reveal financial details or access your email and social media accounts when using public Wi-Fi hotspots. Cybercriminals can hack the connection and intercept your personal and financial information.

Instead, try to use your mobile's data services such as 3G or 4G instead of public Wi-Fi wherever possible. If you must use public Wi-Fi, confirm the connection details with an employee of the organisation providing the free service.