Don’t become the Christmas turkey!

The popularity of online shopping continues to grow every year as consumers discover the savings that can be made in comparison to traditional brick and mortar retailers, and the fact that we can enjoy the comfort of shopping from our own homes and not have to battle the seasonal queues.

However shopping on the web is not always a perfect experience as many consumers discover to their cost.

Last year the National Fraud Authority in the UK received more than 10,000 reports of online fraud and auction site scams over the Christmas period. On average, the victims of these crimes lost over £1,700 each. Of course this is not limited to the UK as on-line shopping fraud is a global problem and the greatest risks are in the lead up to Christmas.

Everyone is searching for the best deals during the holidays. So keep your eyes peeled (and your wallet in check) when online shopping for this season’s most coveted products. Dangerous links, phony contests on social media, and bogus gift cards are just some of the ways scammers try to steal your personal information and ruin your holiday cheer.

Safe Communities Algarve (SCA) has researched some of the most common types of frauds and scams to help you, your family and friends over this period, so please pass on. Our 12 Christmas scams list is as follows.

Phishing scams - Fraudsters send you a message and attempt to make you click on a link to a fake site or open some malware that infects your machine. Imagine you are placing orders on a well-known website for gifts. Suddenly you receive an email - apparently from that very site - saying that there is a problem with your last order and can you please "click here" to attend to the problem. Logos, email addresses, even the link might look genuine but you'll get more than you bargained for if you do as the email asks.

Fake charities - The festive period encourages many of us to think of those less fortunate than ourselves and can prompt generous donations to charities. Cyber criminals take advantage as always. Watch out for fake charities using copied texts and logos in emails or on websites, and check the sender's email address – some fake charity branding can look almost identical to authentic ones – so be vigilant.

Weight loss Scams - Many of us make resolutions to lose weight after indulging at Christmas, but watch out for scammers offering ‘miracle’ weight loss pills and potions. These scams may promise weight loss for little or no effort or may involve unusual or restrictive diets, ‘revolutionary’ exercise or fat-busting devices, or products such as pills, patches, or creams. Also watch out for 'free trials' that may sign you up to unexpected

payments. Be very careful about offers for medicines, supplements or other treatments: always seek the advice of your health care professional.

Parcel delivery scams - If you are expecting a parcel from family or friends, it's important to be aware of scams involving parcel collection. Scammers may call or email pretending to be from a parcel delivery service, claiming that a non-existent parcel could not be delivered to you. They will offer to redeliver the parcel in exchange for a fee and may also ask for personal details. If you are in doubt about the authenticity of a parcel delivery call or email, don't commit to anything. Call the company directly using their official customer service number to verify that it is genuine.

Dangerous E-Season Greetings - Even electronic greeting cards can contain malware (malicious software) that makes itself at home on your tablet, phone or computer when you click on an e-card link. While most are safe and harmless, it is safest not to open the link unless you know the sender. You can also check the address that the e-card came from to verify it belongs to a legitimate, known greeting company.

Holiday job offers – This scam has been seen on social networking site Twitter, where links are posted to high-paying, work-at-home jobs. The fraudsters ask for personal information, such as your email address, home address and other personal details in order to apply for the fake job.

Lottery scams - There are many legitimate lottery jackpots, competitions and sweepstakes throughout the festive season, however lottery scams also circulate at this time of year. These scams will often use the names of legitimate overseas lotteries or carry the name of a well-known company, event or person. If you receive a letter, email or SMS out of the blue claiming you have won a lottery which you never entered it's most likely a scam – ignore it.

ATM Skimming - During the holiday season, you need cash and are usually in a rush to get it. Criminals can access your information at ATMs by installing skimming devices to steal the data off your card's magnetic strip and either using a video camera or keypad overlay to capture your PIN. A simple solution: look carefully at your ATM for anything suspicious and cover the keypad when entering your PIN.

Christmas jokes - As the Christmas spirit gets going many of us send each other links to jokes and videos, on Facebook, by email and via Twitter. Now imagine you arrive at one of these sites and it tells you that you don't have the latest Flash Player so you can't watch that funny video, but not to worry click here and you can get your upgraded player immediately. Not only will this "upgrade" be malware but that malware will go on to send messages to all your friends telling them to go see the "funny" video.

Fake virus checker - You search for that elusive gift, and finally you're led to a site that appears to sell just what your nearest and dearest want. But wait, a message flashes up saying that your machine is infected… but don't worry just download the free virus check shown and your problem will be solved. By downloading it you will actually be infecting your machine and your problems will only just have begun. Install a good virus checker before you go online.

“Help! I’ve been robbed” scam - This travel scam sends fake distress messages to family and friends requesting that money be wired or transferred so that they can get home. McAfee predicts this scam could rise during the busy travel season.

Lastly please take care of your smartphone. With an increase in travel, activity (and bubbly!) over the busy holiday season, people are more likely to forget their smart phones in public places. While inconvenient for them, it is also way for hackers to access sensitive personal information and business data if the appropriate security measures are not in place.

Posted 3rd December 2014