Don’t let scammers ruin your Christmas

In the lead up to Christmas millions of us will go online to buy presents for friends and family, search for holidays, book tickets for a big gig or send an electronic Christmas card. What many do not realise is the hidden threat we now face from criminals online. They are targeting internet shoppers with scams which, on the surface promise to save them time and money, but in reality only deliver festive heartache and misery. Tens of thousands of people sadly fell victim to an online fraud in the weeks leading up to last Christmas and even more are at risk of suffering the same fate this year – being left hundreds, and sometimes even thousands of euros out of pocket with no presents to give on the big day and their electronic devices corrupted with a computer virus.

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

Last Christmas in the UK, almost £16.5 million was lost to online fraudsters - a 42% increase on the Christmas of 2013. 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.

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 10 Christmas scams list is as follows.

Donating/romance fraud - Many singletons will be making a New Year’s resolution to find their ideal partner and signing up to an online dating website. This can be a great way to find true love but you also need to be on the lookout for fraudsters trying to win your affection and then asking for money to pay for them to visit you or help out with a family problem. Do not listen to promises of repayment – better to sever contact and look elsewhere. Guard your privacy when chatting online and be selective with the information you provide about yourself. • Never send money or give credit card or online account details to anyone you do not know and trust. • Trust your instincts.

Ticketing fraud - Creating wonderful memories is a part of the magic of Christmas and what better present to give than tickets to a rock concert or a sporting event? However, there are many bogus websites offering fake tickets. A tried and trusted formula for fraudsters is to offer cheap deals for tickets to events that have already sold out. In reality the tickets do not exist and anyone who tries to buy one will end up losing their money and a memorable day or night out. Only book tickets from reputable websites that are secure and

before buying do an internet search for reviews on the gig/sporting event to see if anyone has fallen victim to a ticketing scam.

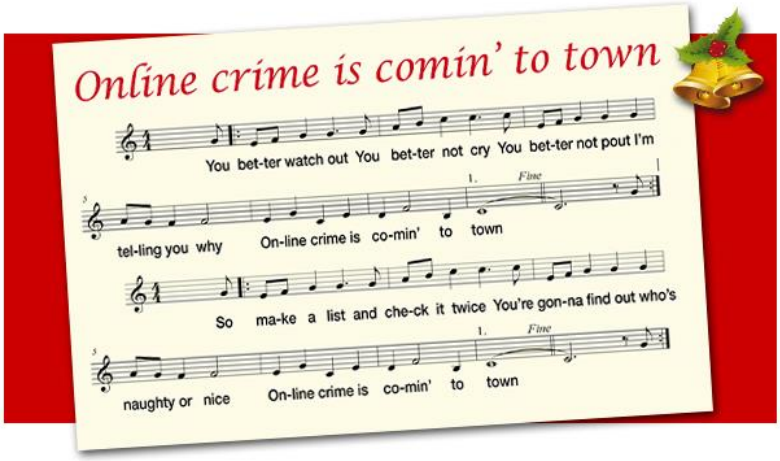
Fake charities - The festive period encourages many of us to think of those less fortunate than ourselves and can prompt generous donations to charities. Cyber criminals take advantage as always. Watch out for fake charities using copied texts and logos in emails or on websites, and check the sender's 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. While many adverts make attractive weight loss claims, the fact is many unlicensed slimming pills simply do not work and can contain dangerous, unknown ingredients."

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.

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.



Holiday Fraud - During or just after the festive period many people are keen to take a few days away, often in search of some sunshine or snow. With the expense of buying Christmas presents most will be going online on the look-out for a deal. However, it is important to be aware of fraudsters advertising fake holidays on websites or social media. These often come in the form of cheap 'too good to miss' package trips, bargain-booking offers for villas and ski chalets or calls and texts offering tempting last-minute deals. Always pay with a credit card; if they don't accept don't buy from them. • Use companies that are ABTA or ATOL protected. • Research the internet and consider the reviews of the company/person you wish to use before booking your trip.

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.

This year, make sure you don't get conned out of Christmas, by thinking twice before you click and taking some simple precautions. That way, you can make sure it's a festive season to remember...for all the right reasons.

Posted 7th December 2015