“Tis the Season to be Jolly”

Yes it is this time of year again, when fraudsters take advantage of the season to be jolly, by lining their pockets at your expense. There are an increasingly number of on-line scams and unfortunately many people fall for these. Good news is that most of these can be avoided by taking the following tips. After all, Christmas can be an expensive time and the last thing we want, is to lose money through a scam.

Firstly the tips the first message I would like to get across is, that not everything on Facebook and other social media is true! There is temptation to respond immediately to posts, and this applies to offers of goods and services. Remember if it appears too good to be true then it usually is! Take time to check any offer out particularly if it means spending a lot of money.

On Line Shopping Fraud

If possible use online retailers/brands you are aware of and trust. For major brands always go to their official website to find a list of authorised sellers. Having selected your retailer then check the delivery, insurance, warranty and returns policy. Another useful tip is to ensure you have adequate anti-virus software that will enable your computer to flag any untrustworthy sites.

Christmas e-cards

If you receive an anonymous e-card, better to play it safe and delete the email as it could be infected, which could then corrupt information on your computer. The risks can be reduced by using a reputable anti-virus product on your electronic device, making sure it is regularly updated and always turned on.

If you believe your electronic devices has been infected, switch it off and disconnect from the internet to prevent further information being stolen. Also contact your bank and change passwords and usernames.

Holiday fraud

Many of us will be taking holidays over the Christmas and New Year periods. Regardless of the service you are using e.g. flights, hotel or car hire bookings, always pay with a credit card; if they don't accept do not buy from them. It is advisable to use companies that are ABTA or ATOL protected. Verify this protected status by contacting the Civil Aviation Authority.

Research the internet and consider the reviews of the company/person you wish to use before booking your trip.

Ticketing fraud

There are some great shows this time of the year. It is wise however only to book tickets from reputable websites that are secure (showing a padlock) and before buying do an internet search for reviews on the event to see if anyone has fallen victim to a ticketing scam. As with any service avoid entering your bank or credit card details on public or shared computers, as the details can be “seen”.

Donating to charity

The big one! Unfortunately the number of fake charity scams are increasing tugging on your heart strings at this time of the year. Never click on a hyperlink in an email purportedly from a charity. Instead visit the charity's website first by typing the address into your browse.

Before you donate, check the website you are on is secure - the web address should begin with https:// (the "s" stands for "secure") and look for the padlock symbol. It is very risky to respond to requests to donate through a money transfer company such as Western Union or MoneyGram. This is the same for any service. If you are still worried, a legitimate charity will advise you on other ways to give on their website or via a phone call.

Mobile malware/malicious apps

There are many of these around. Make sure you have the latest versions of software installed for increased protection. To be safe only download apps from official app stores like Google Play and Apple Store and always check reviews and ratings as well as developer information before downloading a new app.

Money transfers

The best advice to avoid being a victim of fraud is not to send money transfer for online purchases. Wait the six or seven working days it takes for a cheque to clear before transferring any money or sending/mailing any goods. Doing this will mean you don't lose anything even if the cheque bounces, proves to be fraudulent or is cancelled. Never send money in advance to obtain a loan or credit card or to pay for "processing fees" on lottery or prize winnings.

Social media scams

There is no doubt that many frauds take place because the victims have divulged too much personal information about themselves on social media. I always think this is ironical; as people are more worried about Government having too much information about them, but at the same time give more away themselves to the general public. Therefore it is sensible not to have too much personal information on social media accounts which could allow your bank accounts to be compromised.

Dating fraud

On line dating companies report an increasing number of clients at this time of the year. Be very careful regarding the release of your personal information as it may end up the other side of the world in the hands of a fraudster. Guard your privacy when chatting online and be selective with the information you provide about yourself. Be very cautious even after some months after starting an on-line relationship, if you are asked to send money. Fraudsters are prepared to wait a long time before making this pitch, just awaiting the right opportunity. Never send money or give credit card or online account details to anyone you do not know and trust. At the end of the day trust your instincts, if something feels wrong take steps to protect yourself.

Mobile payments

There are an increasing number of services such as banking services available through your mobile device. Security experts believe in the next 2-3 years the number of attacks on mobile phones will exceed that of computers. Sound advice is not to store or save passwords or personal/financial data on your mobile device unless it is absolutely necessary and make sure the phone is passcode protected.

If stolen, most mobile devices have the software to wipe all data from their memory remotely - learn how this works. Do not leave your Bluetooth on as cyber-criminals can hack into your device unnoticed. Also install anti-virus software and check the security features.

I know it is awful at this time of year to even have to think about these matters; but we live in a real world and unfortunately there are those who take advantage at this time of year to carry out these scams and many others. More information about these can be found by visiting www.safecommunitiesportugal.com Cybercrime

Safe Communities Portugal wish you all a Very Happy and Safe Christmas and New Year.

By David Thomas

Algarve Resident Feature

2nd December 2016