XMAS SCAMS

With presents to buy and money to spend, sadly Christmas can be a boom time for scammers who want to have a merry festive season at your expense.

Here are the 12 Christmas scams to watch out for when browsing, clicking and buying online.

1. Mobile app scams

The festive season often prompts the launch of new mobile apps, promising to make Christmas shopping easier. But shoppers should think twice about downloading official-looking software, as apps can carry malware designed to steal personal data. Stick to official app stores for safety.

2. Text scams

Should your mobile number get into the wrong hands you might be exposed to a text scam.

A crafty crook can send text messages promising free gifts or prizes. But following the link might encourage you to share personal details that can leave you exposed to identity theft, or ask you to download something that contains malware that infects your device.

Keep your mobile phone number private and an eye on your phone bill for unusual charges to combat this scam.

3. Gift scams

Adverts with offers on must-have items like the new iPad Mini 4 are sure to attract Christmas shoppers. Cyber fraudsters will post links to fake competitions using social media or send phishing emails offering great deals to get people to reveal personal information or download malware onto their devices.

If a deal seems too good to be true, then it probably is! Be suspicious of really low prices and avoid stores you've never heard of.

4. Festive travel scams

Travel is a big part of the festive period and many will be looking for the best deals online. Cyber thieves are well aware of this and use bogus offers for great deals to trick bargain hunters into entering credit card details and other private information.

According to the National Fraud Intelligence Bureau (NFIB) there were over 1,500 holiday scams reported in Britain last year, costing holidaymakers more than £2.2 million. Again be wary of unrealistically low prices on flights, rental cars and hotel rooms and only use reputable travel sites.

5. Dangerous E-card greetings

E-cards are a fun and cheap way to send season's greetings to family and friends. But scammers are able to send fake versions that contain ‘merry malware’ such as Trojan and other viruses.

These infect your smartphone, tablet or computer when you click the link or attachment to view the greeting. It’s better to be safe than sorry so don’t open an e-card if you don’t know the sender.

6. Deceptive online games

Downloading games for your computer, smartphone or tablet could be another source of misery over the festive period. Many sites offering full-version downloads of games can be laden with malware and social media pages can expose gamers too.

Stick to safe, well-known app stores when downloading games and check online for reviews beforehand for warnings from less fortunate gamers.

7. Shipping notification shams

Ordering things like gifts and food online means you’ll be getting plenty of shipping notifications, so beware fake emails asking you to update your details. These can carry malware and other harmful software designed to infect your devices.

Retailers never normally have to contact you about your details. You should be on the lookout for email addresses that aren’t quite right, as well as spelling and grammar mistakes.

8. Bogus gift cards

If you’re planning on buying a gift card for a loved one, make sure it’s official. Gift card deals are sometimes promoted via ads on Facebook, Twitter and other social sites.

These third-party websites might be selling bogus gift cards that will leave the recipient red-faced when trying to cash it in.

You're better off going direct to a retailer.

9. Holiday SMiShing

Mobile phones and tablets come with the risk of SMiShing or text message phishing.

Scam artists pretend to be banks or other organisations that require your personal information urgently for ‘security purposes’ to avoid an account lockdown or other dire consequences. Some even include the first few digits of your credit card number in the SMS message to lull you into a false sense of safety.

Instead of replying you should contact the organisation directly if you have any concerns.

10. Fake charities

The festive season can move people to help those who are less fortunate, but scammers are on hand to take full advantage of this generosity, setting up fake charity sites to pocket donations. Be on the lookout for bogus charities using copied text and logos in emails or on websites.

Most use a name, email address or web address that is almost identical to a real charity, so it's easy to be caught out.

11. Romance scams

Cyber criminals can use photos, emails and even text messages to pretend to be a member of a dating website. Messages may contain phishing scams where the person can access your personal information such as usernames and passwords or worse your device might get infected by malware.

To avoid this fate only use reputable dating sites, be on the lookout for fake profiles, and never click on links from someone you don't already know or trust.

12. Phoney e-tailers

If you plan to do most of your Christmas shopping online, beware of fake websites posing as legitimate retailers. Brand protection specialist MarkMonitor revealed that nearly a quarter of shoppers looking for a bargain online have been duped by fake sites.

You should check names and web addresses carefully for subtle differences that indicate the site is a fake and wherever possible limit your shopping to known and trusted names.