Tips for shopping online safely this festive season

Online retail is a huge business today, with an increasing number of consumers across the world turning to the internet to buy products and services. There are several reasons for this, but the obvious ones are convenience, affordability and range of choice that physical retailers cannot hope to match.

However, as with any popular online activity, e-commerce has captured the attention of cyber crooks. “Cyber-criminals can be likened to pickpockets. They go where they can find the crowds, and this is why online transactions are becoming a popular target,” says Robert Brown, CEO of DRS, a Cognosec company.

“With that in mind and conscious that the Christmas season is just around the corner, we have assembled a list of tips on how to stay safe and secure when shopping online,” he adds.

Firstly, stick to brands and businesses that you know well, and have a good reputation. In this way, not only can you can be sure you will receive a quality product, but reputable brands and organisations who sell online are sure to have good security solutions and tools in place to protect their customers when shopping online.

“Be careful though. Today’s cyber-criminals are very cunning and clever, often creating fake websites that look so close to the genuine article, they would fool all but the closest examination. After all, this is how phishing attacks have become so successful – these people know what they are doing, and produce extremely high-quality replica sites.”

Brown also advises to shop only on secure websites. “Look for https: rather than http: at the front of the URL. Websites that use https are secure because they employ SSL (Secure Sockets Layer) to encrypt any information that is distributed online, such as your credit card or other login details. In this way, your personal data is kept safe and private.”

Over and above secure sites, Brown advises shoppers to be vigilant in terms of the connection they are shopping over. “Public Wi-Fi is a notorious means for cyber-criminals to carry out man-in-the-middle attacks. During these attacks, the hacker secretly relays and possibly alters the communication between two parties who think they are communicating directly with each other. Public Wi-Fi might be cheap and easy to use, but it isn’t safe. The risks far outweigh the benefits, and public hotspots can be hacked far too easily.”

Payment security

He says it is also a good idea to use secure payment services such as PayPal, and if this isn’t an option credit cards rather than debit cards to purchase goods online. “Payment services are the most secure option. The major advantage is that they act as the middleman. Your payments go to them, and they pay it on to the retail partner. Retailers will never actually see your bank details. Credit cards – more often than not – make use of two-factor authentication, and are more secure than debit cards, and don’t link to money that you really own. Moreover, many credit card companies limit your responsibility to pay back money in the event you are defrauded online.”

In addition, he says to be aware of the old maxim “‘if something seems too good to be true, it probably is”. “Often there are fantastic deals and offers that are totally legitimate, but this isn’t always the case. When you see an offer to buy something fantastic for what is a small fraction of the usual price or value, beware. Many scams promise unbelievably good offers as a means for sucking their victims in, when in reality, they are hoping to infect their targets with malware. Be careful. If the site isn’t well known, if there’s no SSL showing, then rather err on the side of caution.”