# eShop, but don't drop (your guard)

Protect your identity and finances as you hunt for that perfect gift online.

By HARIATI AZIZAN
sunday@thestar.com.my

THE holiday season is here, and for many, that means the arrival of the shopping season too!

Malaysians' love for shopping could not have found a bigger outlet than the World Wide Web store, with the help of their very own personal shopper – their mobile device.

It is no wonder retail apps and local online shopping have seen a boom. But as you e-shop to your heart's content, don't do it until you drop all your defences, warns safety giant Symantec Corporation. Cyber criminals are also getting a lot of joy this festive season, having a merry time pouncing on the unaware and careless.

Here are a few e-shopping safety tips to protect yourself as you hunt for that perfect gift. Don't let the time you save on travelling on jam-packed roads, fighting for parking spaces and waiting in the long cashier lines be wasted queuing at the police station.

**Don't be too "App"-y:** Think twice before downloading unknown apps from third party app stores. They could come bundled with malicious software or adware. Also, read the permissions the app requires carefully before downloading.

**Think before you click:** Have your guard up for email and text advertising holiday deals that seem to good to be true. No matter how harmless a spam looks, avoid clicking on the links and downloading the files if you don't know the sender.

**Beware the friendly reveller:** Even if the mail makes your day with its cheery message: "You have received a Christmas Greeting Card!" or "Cash for the New Year", check before you open it. Norton has found some of these holiday mails to contain viruses and worms that will damage your computer, or worse, send you and your children to websites designed to steal your bank account details.

**Look for the 's':** To make sure you are shopping from secure sites, look for the "s" after "http" in your browser address bar before providing personal or credit card information. Whether shopping from a smartphone, tablet or home computer, only use reputable retailers and websites.

**Secure your phone:** Your phone now is also your wallet these days, so take precaution with a mobile security solution to protect your phone no matter where you shop, surf or share.

**Be "cheap" with your credit card:** Use one low-limit credit card for all your online transactions so that if you become the target of a cyber attack, you won't find yourself crying over thousand-ringgit losses.

Use a credit card instead of a debit card. It will be easier to stop payment or cancel purchase if you use a credit card. A debit card's payment is made directly from your bank account and is difficult to reverse.

**Ignore the pop-up:** Don't click on the pop-up advertising, even if it promises gift cards, cash or discounts if you fill out a survey. It's better to be safe than sorry, so use Control + F4 (Windows) or Command + W (Mac) to close the pop-up ad.

**Think before you click:** Retail apps and local online shopping have seen a boom. But as you e-shop to your heart's content, don't do it until you drop all your defences.

**Don't do your business in public hotspots:** When you are shopping on the go, free WiFi can be tempting but security for such connections is usually lacking.

To avoid any disappointing surprises, steer clear of unencrypted, public hotspot network connections when buying things online. Cyber criminals might be monitoring the public network for online shoppers' credit card information.

If you really need to use the public WiFi hotspot at a coffee shop,

> TURN TO PAGE 26

# A season of joy – for cybercriminals too

> FROM PAGE 25

mall or even hotel for important transactions, make sure it is secure.

**Read the fine print:** Always read the terms of service agreement before you buy online. You could inadvertently sign up for subscriptions or get hit with additional fees or restrictions.

**Beware the fake charities:** Going on a shopping spree might trigger your guilt and make you easy prey to charity hoaxes. There are cyber criminals using fake requests to access your device and exploit your personal information. Before making any donation, confirm that the charities in question are legitimate.

**Hide the box:** After your goods have been delivered, especially the expensive electronic items, wait until rubbish collection day to put the boxes out. Don't "advertise" the empty boxes outside your house – you might get unwanted guests.

**Avoid holiday oversharing:** If you are using the holiday package or airline ticket you bought online this holiday, don't overshare it on social media. Adjust your settings and limit geo-tagging of photos and posts so that only trusted friends can see your whereabouts.

**Watch your device:** Your banking or credit card details and identity are not the only "gifts" cybercriminals are shopping for; your smartphone and tablets are also hot items. Apparently, the lost and stolen mobile device market is booming too.

Password-protect your phone with a code that is difficult to crack. Install software that will allow you to track, lock and wipe your device if it's lost or stolen.

*> Source: Norton eShopping Safety Guide and Savvy eShopping Tips by Symantec, USA.gov*