Shop Online Securely (SOS) this Lunar New Year with Security Tips from Kaspersky Lab

Every festive season turns into a shopping frenzy, and the action has moved increasingly online. With the convenience of online payment and in-app purchases, with delivery to your door, comes the very real risk of cybercrime, with you as the target.

Everyone loves a great deal during the Lunar New Year, and throughout the year. For cyber criminals, your frenzied shopping to get all the items you need delivered before the festivities begin is a prime opportunity. This is because in the euphoria and adrenaline rush of shopping, you will be more likely to make basic mistakes that can expose your personal data.

General Manager for Kaspersky Lab Southeast Asia, Sylvia Ng explained that the brand understands festive season shopping is a priority for consumers but reminds that it is also a prime opportunity for cyber criminals. “Get your shopping done safely. Sipping on an espresso at a local coffee house and doing your Internet shopping does seems convenient. However, you open yourself up to criminal activity by doing so. Public Wi-Fi networks are often less secure than private ones, and you risk the possibility of logging onto a phantom network instead of the real one, opening you up to potential identity theft”.

Everyone needs to be wary of public Wi-Fi when using your smartphones and tablets. If you have to do your shopping on any Wi-Fi network, you first need to ensure that it is secure and a network you can trust. Cyber criminals know consumers are more likely to visit sites with login accounts or financial information during busy shopping times. They can easily monitor all the information sent across public Wi-Fi networks, which can include your bank account or credit card number. Is that deal really so attractive that you are willing to put your online identity and finances at risk? Probably not.

This year, don’t let your last minute shopping frenzy lead you down a path of bad security decisions.

Here are some common mistakes, and how you can avoid them.
- Check that you are using the authentic website of your bank or payment system – this should be obvious, but it is a common mistake that can be very costly!
- Pay attention to the https prefix, which indicates an encrypted connection – makes a world of difference.
- Check the spelling of the website – a misspelled address is an obvious sign of a fake phishing page.
- Use that virtual keyboards to protect your password from being intercepted by key loggers.

Also, consider the following when shopping online:

Avoid ransomware — don’t open email attachments from unknown shopping sites, and always back up your files.

Be aware of phishing links — don’t click on unexpected links sent via email, SMS, or messengers.

Create strong passwords — combine letters, number and special characters to make them harder to hack. (give it a try on our password checker : https://password.kaspersky.com/)
Shop at safe sites — browse reviews before trusting online shopping sites with your credit card info.

Avoid shopping on public Wi-Fi — criminals love to snoop for your credentials in unsecured wireless networks.

Turn off Bluetooth, connect via cellular — these simple steps will make your smartphone connection much more secure.

Deny suspicious freeware — these ‘gifts’ might include adware or something even worse.
Avoid forged shipping confirmation emails — it could be a phishers’ bait for a quick click.

“These tips that we share are culled from real-life experiences of people. So, before you click on any deal, make sure that you are going to trusted sites. If you find a deal that seems too good to be true, it probably is,” added Sylvia Ng.

Kaspersky Lab wishes you a safe and prosperous Chinese New Year. Gong Xi Fa Cai!