


IT'S HOLIDAY SEASON! STAY SAFE WHILE ONLINE SHOPPING

It is the holiday season again, festivities, family gatherings and holiday shopping! Cybercriminals don't take the holidays off, they are constantly looking for easy targets. While legitimate businesses are after your money, so are cybercriminals. You probably receive a "potential spam" robocall, an email with a mysterious link, or something in the mail claiming you've won a prize on a regular basis. With the increase in online shopping, cybercriminals grab the opportunity to make more money with fraudulent phishing emails, scams and fake websites. With the ever-increasing number of data breaches exposing your personal information and payment card data, it's never been more important to stay vigilant. Watch out for the scams below!

- 
1. Gift card scams including empty gift card.
 2. Lookalike online stores.
 3. Phishing emails from companies you trust.
 4. Fraudulent seasonal jobs.
 5. Package delivery scams.
 6. Social media ads promoting fraudulent items.
 7. Popular holiday feature too good to be true prices.
 8. Holiday travel and online airfare scams.
 9. Fake online giveaways and surveys on social media.
 10. Scam online gift exchange. E.g. secret santa scams
 11. Fake charities that steal your money.
 12. Hacking over public WiFi.
 13. Shoulder surfing and card skimming while shopping.



General Helpline: help@securitymatters.asia
Secure Communication via Protonmail:
secmhelpdesk@pm.me

More information about Security Matters,
visit www.securitymatters.asia

 info@securitymatters.asia

 @secm8

 @sec_matters

IT'S HOLIDAY SEASON! STAY SAFE WHILE ONLINE SHOPPING

Tips for safe online shopping



Use strong passwords. Do not reuse password across sites. Enable two factor or multi factor authentication 2FA/MFA.



Only download shopping/e-commerce app from a certified app store.



Only shop from trusted retailer websites. Verify the validity of the website and check their reviews.



Avoid clicking links and attachments in emails and texts from unknown senders.



Make sure your shopping sites are legitimate and secure. Verify the sites by checking the green "padlock" symbol in the URL bar and the URL should start with "https".



Keep your device updated and patched. This includes your web browser, anti-virus software, and operating system.



Beware of fake websites that offer deals that are too good to be true. Double-check the market prices directly with the official retailer. Ensure that the e-commerce sites are legitimate, have a clear product description and check their reviews.



Avoid direct purchase via WhatsApp, Facebook, and other social media sites. Verify information before sharing on social media.



Never make purchases on public WiFi. If you need to, be sure to use a Virtual Private Network (VPN) to encrypt your traffic.



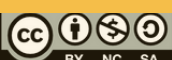
General Helpline: help@securitymatters.asia
Secure Communication via Protonmail:
secmhelpdesk@pm.me

More information about Security Matters,
visit www.securitymatters.asia

 info@securitymatters.asia

 @secm8

 @sec_matters



IT'S HOLIDAY SEASON! STAY SAFE WHILE ONLINE SHOPPING



Avoid connecting devices to public charging stations such as in stores, airport, hotel, cafe, etc. If you have to, use a USB data blocker instead.



Beware of charity scammers. Verify charities before donating.



Always check the privacy policies of the shopping sites to make sure your information is safe.



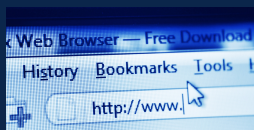
Read and understand the terms and conditions of purchase before you make it.



Use a secure payment method. Pay with a credit card instead of a debit card. Opt for cash on delivery if possible.



Monitor your bank account and credit card activity.



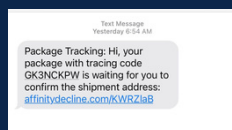
Avoid saving your information while shopping online. E.g. username, credit card info, passwords in your browser. Clear your browser cookies and history regularly.



Be careful with phone calls. If you receive an unsolicited calls from someone claiming to be from your bank or credit card company, do not provide them with any personal information.



Monitor the shipping process. Always get tracking numbers for items you buy online. Inspect your goods as soon as they arrive and notify the seller immediately if there is any problem with them.



Beware of fake delivery or shipping notifications scams. Think twice before clicking in shipping notification email/text. Always verify the company before provide your information.



General Helpline: help@securitymatters.asia
Secure Communication via Protonmail:
secmhelpdesk@pm.me

More information about Security Matters,
visit www.securitymatters.asia

 info@securitymatters.asia

 @secm8

 @sec_matters

Related News

Parcel delivery scams re on the rise: Do you know what to watch out for?

E-commerce has never been easier. In just a few mouse clicks or swipes of our smartphone, we can have items from all over the world delivered to our doorstep. But this ease of use can also be our undoing. Scammers are primed to take advantage, by sending out phishing emails and texts impersonating delivery companies, which claim something is wrong and urge users to click through. [Read more: https://bit.ly/3NPK3Ph](https://bit.ly/3NPK3Ph)

Trick or treat? Stay so cyber-safe it's scary – not just on Halloween

Hackers, imposters and scammers of all ilk are looking for you in all corners of the internet, and all they want is to trick you into giving away your personal data or money. It's a good time to look at some common ways your personal information could be at risk (not just this Halloween!) and offer up some sweet treats to help you and your family avoid falling for hackers' tricks. [Read more: https://bit.ly/3DSzAJs](https://bit.ly/3DSzAJs)

Kaspersky: Malaysia is one of the worst SEA countries to be in if you want to avoid getting scammed

According to Kaspersky's infographic regarding financial-related phishing in the SEA region, Malaysia has recorded in the top two rankings, above Vietnam, Indonesia, Thailand, and Singapore in the first two quarters of 2022. [Read more: https://bit.ly/3DSvVR](https://bit.ly/3DSvVR)

Tips on how to spot online scams and protect your digital footprint

As the Internet makes it easy for this information to 'travel,' it is vital for consumers to safeguard their digital footprint. Practicing safe online habits and managing personal data can help consumers to be less susceptible to cybercrimes, such as fraud, which results in financial losses and personal data theft. [Read more: https://bit.ly/3UkRTxT](https://bit.ly/3UkRTxT)

New extortion scam threatens to hurt your reputation and steal your data

A new phishing email is making the rounds, targeting website owners and administrators around the world. Media are warning website owners and administrators not to fall for the latest high-profile scam campaign which threatens to leak a website's sensitive data, blacklisted for spam, and damage its reputation. [Read more: http://bit.ly/3VkDzFE](http://bit.ly/3VkDzFE)



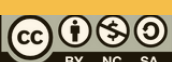
General Helpline: help@securitymatters.asia
Secure Communication via Protonmail:
secmhelpdesk@pm.me

More information about Security Matters,
visit www.securitymatters.asia

 info@securitymatters.asia

 [@secm8](https://www.facebook.com/secm8)

 [@sec_matters](https://twitter.com/sec_matters)



Related News

Beware! Massive YouTube campaign aimed to steal login credentials

There was an extensive phishing campaign that took advantage of YouTube as a vehicle for promoting the download and installation of cracked software and free games. These malicious campaigns mainly target people who are interested in obtaining free software, such as games, programs, etc. in exchange for their email addresses.

Read more: <https://bit.ly/3goNQSU>

Personal data of AirAsia Malaysia, Indonesia and Thailand passengers allegedly leaked due to ransomware

Personal data belonging to 5 million AirAsia passengers via AirAsia Malaysia, Indonesia and Thailand may have been leaked after the airline was hit by a purported ransomware attack. It was alleged that AirAsia was a victim of a Daixin Team ransomware attack and the attackers have shared two CSV files which contain personal details of passengers and employees.

Read more: <http://bit.ly/3ET6wDo>

Watch out for PayPal "money request" scams

A PayPal-branded scam that was reported earlier this week which it would be worth warning others about, especially for those with PayPal accounts who may be more inclined to use them at this holiday season.

Read more: <http://bit.ly/3OpBYw4>

42% of people use their names in passwords

The most common passwords around the world showed that 42% of people use their first name in their passwords, while 43% of them use their birth date. Since this information is easily traceable on social media, your accounts can be more prone to hacking attacks.

Read more: <http://bit.ly/3hS4gTM>



General Helpline: help@securitymatters.asia
Secure Communication via Protonmail:
secmhelpdesk@pm.me

More information about Security Matters,
visit www.securitymatters.asia

 info@securitymatters.asia

 [@secm8](https://www.facebook.com/secm8)

 [@sec_matters](https://twitter.com/sec_matters)

