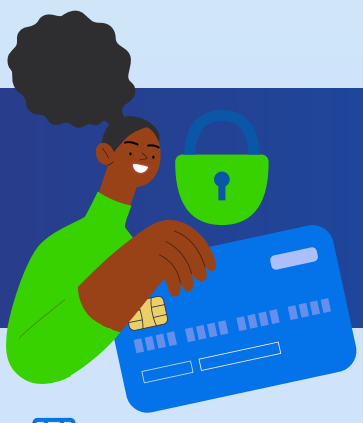
‘Tis the **season to be ready!**

As we get excited for the year-end sales and travel season, so are the cyber criminals. Scams peak during this time of the year as consumers shop around for bargains and are prone to letting their guards down.

Watch out for these common scams and enjoy the festivities with a peace of mind.



Shopping around online?
Remember to only engage and purchase directly from legitimate brands and companies.

Lookalike online stores

Scammers create websites or apps that impersonate legitimate brands with steep discounts to trick people into buying them. Typically, those who purchase can’t reverse their payments or refunds, and more often than not get their credit card information compromised.

Fake product listings

These listings are created on legitimate apps or websites. It’s one thing to overpay for a poor-quality product, but victims may be told to download a malicious app to complete the purchase. Upon doing so, hackers can access sensitive information or takeover the device completely.

Online giveaways

It is common to come across free giveaways or activities online during the year-end festivities. However, scammers often post fake events to lure people into giving up their personal information or share card details for a chance to win a ‘prize’.

Donation scams

People are more likely to donate during the year-end season and criminals exploit this by setting up fake charities online. Whether it’s a paid ad or social media post, people are tricked onto a malicious website to make the donation, revealing their credit card details.

Useful tips

- Verify reviews of an online store by checking against other independent websites, instead of trusting what’s written on their own platform.
- Confirm that a website is safe before sharing your details and making a purchase.
- Avoid making payment if you are taken to a different platform, or via methods that are less secure (e.g. cash transfers, gift cards or cryptocurrency).
- Don’t download a separate or unfamiliar app to complete a transaction.
- Never trust any deal that’s too good to be true, especially if you’re asked to provide personal or financial information upfront in order to be eligible.

After making a purchase, you could receive a delivery update or be contacted regarding problems with your order. But wait, did you actually buy this item?

Delivery tracking

You may receive a message out of the blue informing you of an incoming package, with a link to track its location and update your delivery preferences. When clicked, malware may be installed onto your device or you may tricked into giving up personal data.

Customs payment

Like the tracking scam, scammers send out messages to targets with a link for payment to release a package stuck at customs. People who are expecting a package, like those who bought items during the year-end sale, are likely to fall prey if not careful.

Returns/Overpayment

Scammers also often reach out to customers informing them that they’ve overpaid for an item and a refund is due. But to receive it, account or card information must be shared. People become less wary when receiving as opposed to paying more, and unknowingly fall victim to this scam.

Fake invoice

Scammers impersonate brands and send fake invoices to people. The message will claim your card has been charged or contact them to cancel. Victims are then connected to a fraudulent customer service centre and risk exposing personal and financial information during the exchange.

Useful tips

- Always confirm the delivery and payment status of your orders by logging in to your online shopping account of the website you purchased from.
- Ensure that the sender’s email address of any follow-up notification is legitimate and not spoofed.
- Don’t respond to suspicious messages or emails. Delete and report the incident to the brand or company using a known and trusted channel.

While preparing for your holiday trip, you could potentially become the unsuspecting target of a scam, especially if you’ve been oversharing your plans on social media!

Declined credit card payment

In this scam, customers receive an email or message from the alleged booking company that their card was declined for their hotel or flight payment. Victims are pressured to pay quickly or risk having their booking cancelled.

Cancellation issues

Scammers also contact targets to inform them that their flight or hotel has been overbooked. Victims may be charged a cancellation fee or asked to pay a rebooking fee to confirm a new booking.

Fake customer support

These emails or messages often include a customer support hotline to help resolve the issue. However, these are also part of the scam and by contacting them, victims are often directed to reveal personal and financial information during the exchange.

Last-minute offers

If you’re on the lookout for last-minute deals, be wary of those with steep discounts. These scams typically are hosted on a malicious website or request for payment that are non-protected such as bank transfers, gift card payments or cryptocurrency.

Useful tips

- Double check that the sender’s email address of any follow-up notification is legitimate and not spoofed.
- Be alert if you’re asked to pay more on top of an original booking for any reason. If re-booking is required, it’s usually done without having to pay additional fees.
- If you’re unsure about your booking, contact the airline or hotel directly on a separate and trusted channel to check and report any suspicious incidents.
- Don’t share sensitive information about your booking details (e.g. reference number or credit card information) if someone claiming to be from ‘customer support’ contacts you
- Avoid oversharing your travel plans on social media to prevent cyber criminals from targeting you.