

Fake order scams are increasing

As the holiday season gets underway, we're seeing an increase in fake order scams. These are sent via fake emails detailing an order update or subscription details, and usually appear to be from a well known brand.



Here's what we know:

1. Big brands

Amazon, Paypal, Best Buy, and even Avast are just some of the names being impersonated.

2. They look real

Scammers are innovative — they know how to make these emails look like the real deal.

3. Your money is their goal

They ask you to contact them and demand card details or pressure you to purchase gift vouchers.

What can I do to protect myself?

Keep these 4 tips in mind over the holiday season to help you think twice about what you find online.

Remember these key points:



Even if an email appears to be from a big brand — double check. Cross-check the email address with the official support on the company's website.



Be careful as you search for better deals this holiday season. With the cost of everyday items rising it can be easy to fall for what seems like a great deal.



Never send money, credit card details, or copies of your personal documents to anyone — legitimate companies will not ask for these in that way.



Keep your antivirus software updated and running. Scams like these prey on human weakness — so we need to work together.

Global fake order scam examples



KELLY SWOPE sent you a money request

NOTE FROM KELLY SWOPE:

“ Please Contact Our Customer Support Team Immediately At +44-800-058-4198 If payment Is Not Allowed For McAfee Antivirus Of £1099. 99 GBP ”

Money request details

Transaction ID
U-45487180NK8467502

Transaction date
18 November 2022


Amount requested £1,099.99 GBP

[Pay Now](#)



[Help & Contact](#) | [Security](#) | [Apps](#)



Thank you for your order with us!

Thank you for purchase of yearly package of **Norton LifeLock Premium**.

Your Invoice Id: 723546985206 Date: 10/07/2021

Order Details


Order Id	98756223
Plan	Norton Premium
Amount	\$499.00
Payment Method	Auto - (Card)
Balance Due	\$499.00

Note:


1. If you wish to discontinue the services, please call us within 24 hours. Our support team will be happy to assist you with all your queries.
2. The transaction may take several hours to appear in your account.
3. Please retain this email as your proof of purchase. To obtain information on how to download or activate your product, go here [Norton Firewall/download](#) and please review our "How do I Download?" Help document.

If you didn't initiate this order purchase, or this payment was not made by you, directly reach out our customer support helpline at [1-802-455-8666](tel:1-802-455-8666).

[Support](#) | [Legal](#) | [Privacy](#)



Receipt




Netflix Premium Account
Ultra HD + 4 Screen

Dear customer,
You have made the following purchase with details:

App	: Netflix Premium
Provider Content	: Streaming HD Movie
Date	: Monday, Apr 20, 2020
Items	: 3 Months Membership
Price	: \$19.99
Payment Method	: Credit Card Linked

You get this email to make sure it is you, if you do not make a purchase and or you believe an unauthorized person has accessed your account, You must cancel the purchase as soon as possible, To cancel your purchase within 24 hours after receiving this invoice, [Cancel and Manage Purchases >](#)

Sincerely,
App Store



Copyright © 2020 . Apple Inc.
[All rights reserved.](#)

We hope this has been useful!

Scammers love the holidays just as much as the rest of us. Online shopping habits often increase and people are usually on the lookout for great deals on products and services. Always be vigilant; if something seems too good to be true, or you didn't order it, then it probably is a scam.

From all of us here at Avast, stay safe both online and off.

