Email samples and screenshots in this analysis are from Phishing Pot by Peixoto, licensed under CC BY-NC 4.0. The original sample analysed in this report can be found below:

Phishing Pot: https://github.com/rf-peixoto/phishing_pot
Peixoto: https://github.com/rf-peixoto
License: https://github.com/rf-peixoto/phishing_pot/blob/main/LICENSE
Source file: https://github.com/rf-peixoto/phishing_pot/blob/main/email/sample-5878.eml

Executive Summary
==========
This report analyzes a phishing email impersonating Norton, sent from what seems to be a Google Workspace account. The attacker attempts to trick the recipient into calling a phone number under the pretext of getting a refund for a subscription. Indicators of compromise include urgency tactics, failure of DKIM authentication, non-Norton email and phone number use, and a typo in the attachment. The email demonstrates typical characteristics of payment information harvesting attempts. Defensive actions were taken to block the sender and associated domains to prevent further exposure.

Headers
==========
Date: Wed, 20 Aug 2025 01:06:47 +0700
Subject: Your Norton Order Confirmation For Order #NP00X01062020

To: noreply_emails01062002520@bill.norton-us.com
From: E-Receipt Notice <189.152.152.123.peyja@neo.karenphillips.com>

Reply-To: None
Return-Path: 189.152.152.123.peyja@neo.karenphillips.com

Sender IP: 209.85.216.67 (Google LLC, US)
Resolve Host: mail-pj1-f67.google.com

Message-ID:
<CAABL=kkOdgd2qMioVe7FMDZYcnbVsfVy05pN-N7KHqVg8O5ZnQ@mail.gmail.com>

Phone number: +1 818-282-0908

Attachments
==========
Attachment Name: Billing-Details#NP0045698791324.docx
MD5: 64b2e579fbbead913282aa1c5f846b4a
SHA1: 22c324a2a882307f8f897534f397089971f0790b

SHA256: 2dbb5c169577e34b15a5ea589e877862a599bdfefca9d6978b769f3c0b77aa57

Description
==========
The email claims to be from Norton. It reads that there was an invoice due to an automatic renewal of a $299 yearly subscription service. There are no URLs in the email, but it does have an attachment.

There is an indicator of urgency, as the email suggests to call the billing department within 24 hours.

The email tries to take advantage of subscription confusion. Users often have multiple subscriptions they do not keep track of, and attackers like to take advantage of that.

Artifact Analysis
==========
Sender Analysis:
The From and Return-Path use a domain unrelated to Norton. The attacker tried to obfuscate their email address with the display name “E-Receipt Notice”.

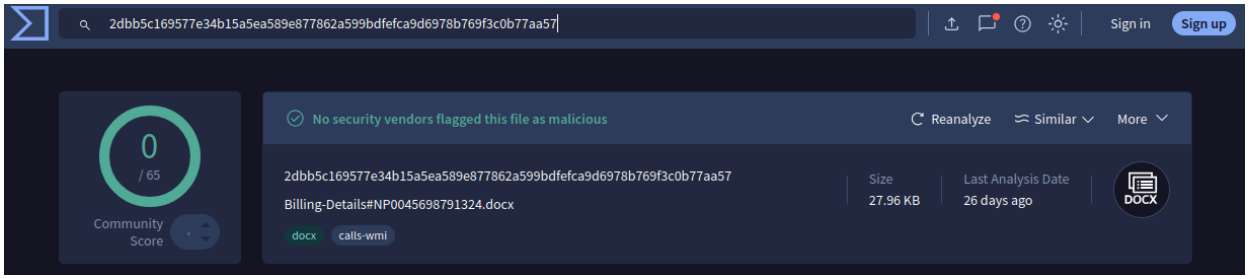
The phone number listed does not match the phone number for Norton’s Billing department on their website.

From the IP address and message-id, it looks like Gmail infrastructure was used. Perhaps Google Workspace, which allows domain customization?

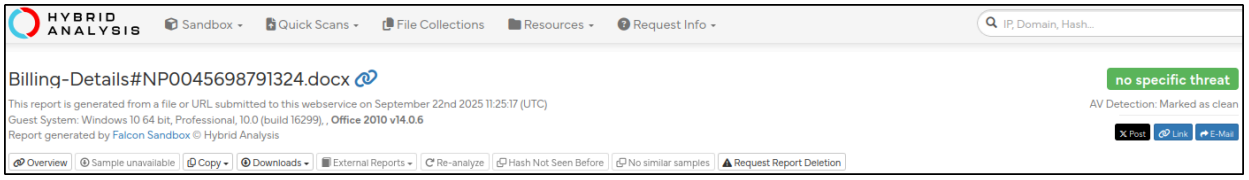
There is an IP address in the From email address, which is strange. An IP in the local-part of an address has no effect on SMTP routing. However, it may a deliberate obfuscation or randomization tactic used to evade filters or make the message look system-generated

The DKIM check failed, so the email address may have been spoofed. However, the DKIM might also just have failed because Phish Pot anonymized information about the email recipient.

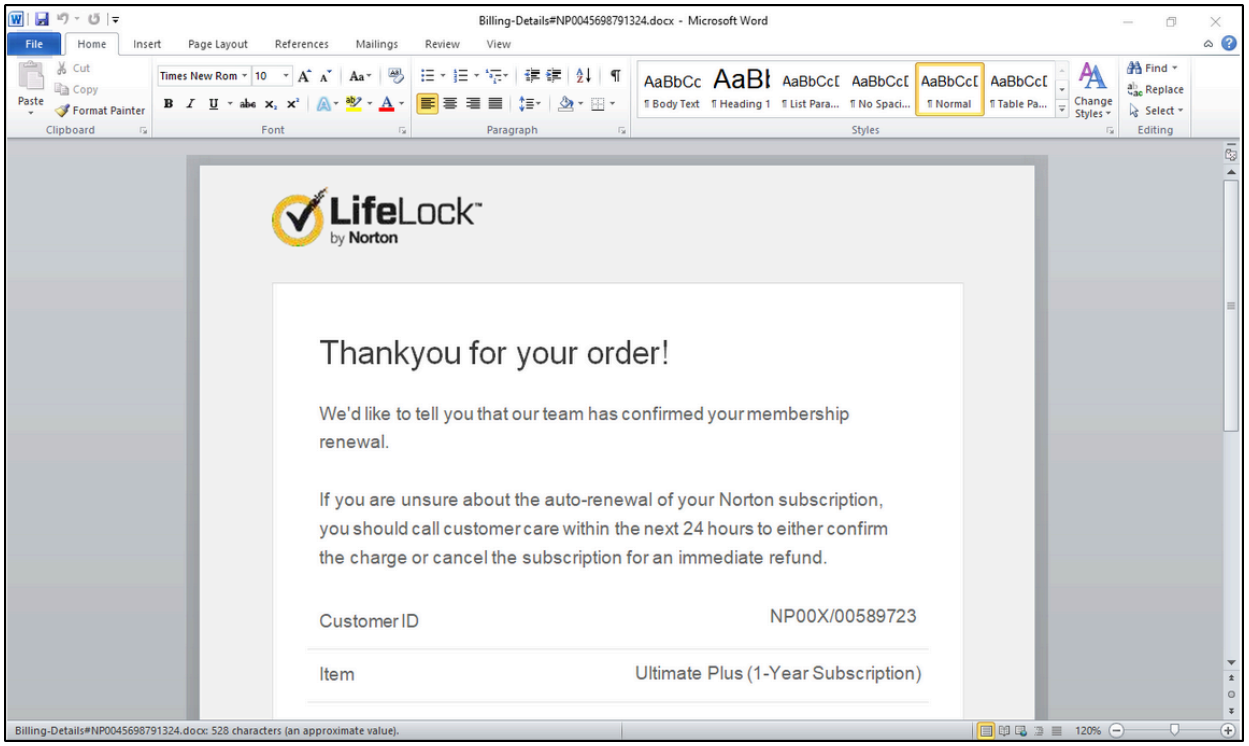
Attachment Analysis:
The file hash of the attachment gives no hits on VirusTotal or TalosIntelligence.



Dumping the file and then uploading it to a Hybrid Analysis sandbox also gives no threat rating.



Looking at the indicators in the report, it all looks Windows Word related. It looks like the file itself may be benign and does not load any macros or scripts, nor are there any URLs in the text file. The screenshots in the report also just display text, with one word having a typo.



Verdict

==========

Due to the sender not being affiliated with Norton, this is a clear impersonation and spoofing attempt. The legitimate Norton service uses the @Norton.com domain for emails.

While there are no malicious URLs and files, since there is a phone number, the goal of this phish may be to have the user call in and to then harvest credentials or credit card information.

Norton's support website warns of subscription renewal scams like this:
https://support.norton.com/sp/en/us/home/current/solutions/v138341527

As a result of the analysis, this email has been determined to be malicious.

Defense Actions

==========

After performing a message trace, no other users within the organization received an email from this sender or with a similar subject line.

To prevent the malicious sender from sending any other email to the organization, I have blocked the "neo.karenphillips.com" domain on the email gateway. The neo.karenphillips.com is not used by any legitimate websites at this time. Additionally, emails that contain the phone number "+1 818-282-0908" or have an attachment with the above mentioned file hashes have also been blocked.

Recommendation

==========

As this email does not show any of the regular phishing tactics that trick users into opening a file or URL, I would recommend adding the following to our anti-phishing training:
- Always look up a company's phone number online instead of using the phone numbers listed in an email.