Email Scams

Scam Overview

There are so, so many variants of email scams. Too many to call out here, so we are going to show you exactly what to check in the email, to help you determine whether the email is a scam or not. This tip works no matter what variety of email scams you receive. Here are just a few recent examples of email scams:

- McAfee Subscription Renewal
- Geek Squad Subscription Renewal
- Venmo Incoming Transaction on Hold

Background of the Email Scam:

The email scam has two components:

- Emotional
- Technical

The **Emotional** element is consistent across most scams:

- Email arrives unsolicited
- Seeks to prey on fear, and/or
- Seeks to prey on unexpected gains (greed)

On the fear side, this can be seen as an unexpected charge against your credit card. Typically the charge is excessively high, normally in the hundreds of dollars. The key to this scam is that it appears to be from a real company such as Amazon, McAfee, or Venmo.

On the greed side, this can be seen as an attempt to refund an amount that did not go through and they need you to contact them. Again, the email arrives from what appears to be a valid, well-known company. We will cover the **Technical** component under the Red Flag Assessment section.

Red Flag Assessment

Domain Names [1]

To understand the technical red flag of the email scam you need to understand the makeup of an email address. Email addresses are divided into 3 parts, for example: **Edward@endelderfraud.org**

1. Originator: In the example, "Edward" is the originator
2. Delimiter: "@" is the standard delimiter to separate the originator from the domain
3. **Domain: "endelderfraud.org" is the domain--the service hosting the email originator account**

For most **major companies** such as Amazon, Venmo, ATT, GeekSquard, and McAfee, **the domain will be the company name**, for instance : @Amazon.com, @Venmo.com, @ATT.com, etc.

An alternative--and more suspicious--domain will be: @aol.com, or @gmail.com, or @yahoo.com. These are email domains that indicate the originator is using a public email host provider versus a specific company. An example of a good vs. a bad/suspect email is:

Good: AmazonOrder@amazon.com

Bad/Suspect: AmazonOrder@gmail.com or VenmoOrder@aol.com

The "Bad" examples reflect scammers that are attempting to fool you into thinking Amazon or Venmo are sending you an email, although the domain reflects the emails are not from Amazon or Venmo.

Please note. There is nothing intrinsically bad with the domain names of aol.com, gmail.com, or yahoo.com. They are wonderful domains for many people, however, **they are not common domain names for major corporations**. So that is why domain names are such a great clue for you if you receive these suspect emails.

Grammar

Although bad grammar and poor sentence structure do not necessarily indicate an email is a scam, they are additional factors you can consider when determining an email's credibility.

What To Do If You Are Contacted:

Email scams follow the same basic principles as all scams reflected in the End Elder Fraud Awareness training sessions, specifically "FEAR" coupled with a sense of "URGENCY."

For email scams, your first reaction is usually the best reaction, specifically surprise and perhaps doubt. Expressed another way, "spidey sense". We recommend the following:

1. Do not click on any links in the email
2. If you feel you need to contact the vendor, look up the official site for the vendor online
3. Call the customer support number given on the official site to confirm the email and issue which has been communicated to you

Examples of “scam” emails (note the domain names)

8/7/22, 9:42 AM [redacted]

Gmail [redacted]

[redacted] **paid $300.00**

1 message

Venmo Pay <venmo.onlinepayserviceee@aol.com> Thu, Aug 4, 2022 at 2:11 PM

To: [redacted]

[redacted] Paid You.

Transfer Date and Amount:

Aug 04, 2022 PDT ·

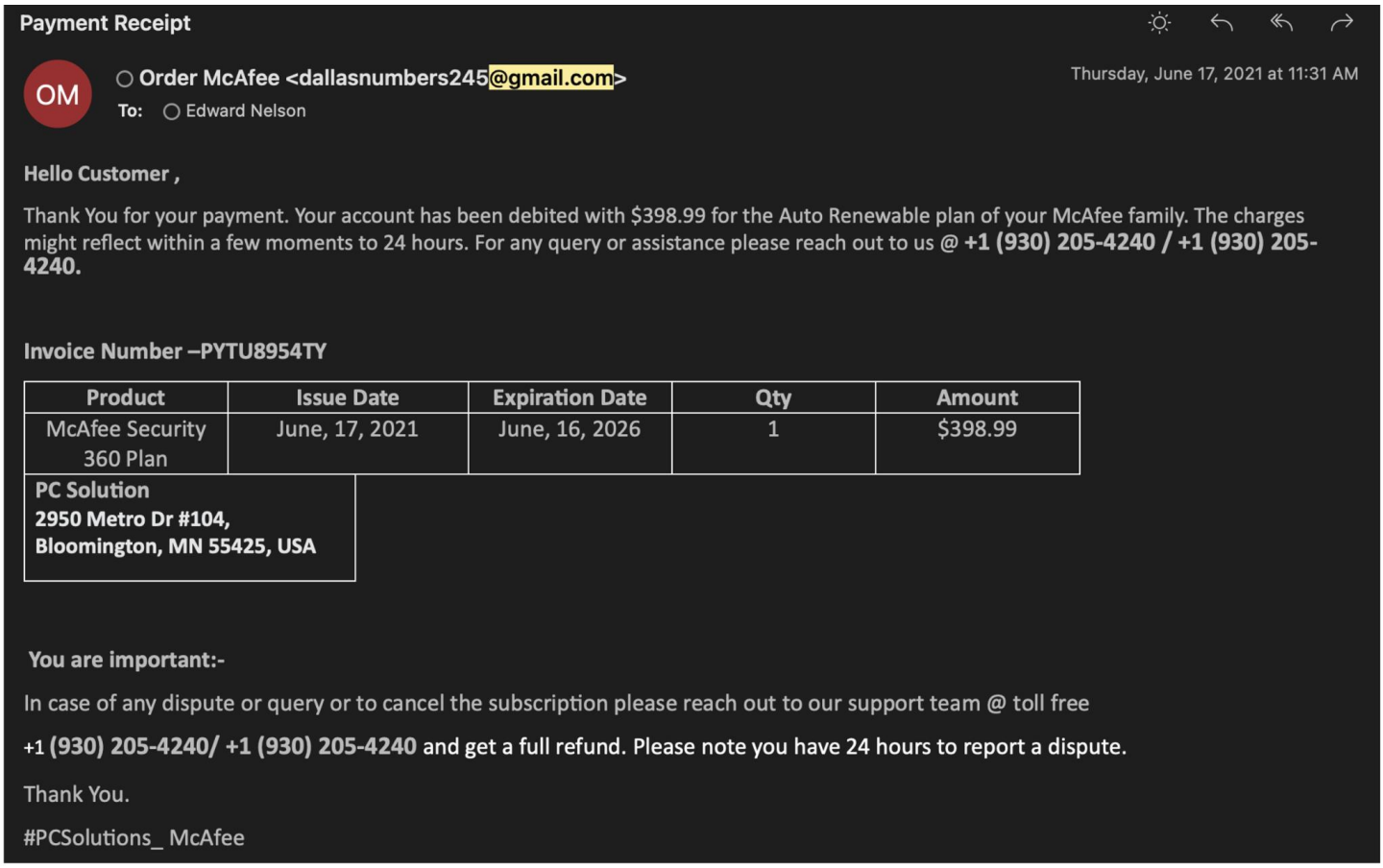
+ $300.00 +Transaction fee ($0.65)

INCOMING TRANSACTION ON HOLD

We have a problem crediting your account with the sum of $300.00 USD because your account have reach it limits. This amount seems to be above your limits so you have to take this urgent step to expand your limit.

To expand your account limit, contact the buyer of your item to send in an additional payment of $400.00 USD into your Venmo account to expand your limit. Soon as this is done, we will credit your account with the total sum of $700.00 USD.

[redacted]



Payment Receipt

OM

Order McAfee <dallasnumbers245@gmail.com>

To: Edward Nelson

Thursday, June 17, 2021 at 11:31 AM

Hello Customer ,

Thank You for your payment. Your account has been debited with $398.99 for the Auto Renewable plan of your McAfee family. The charges might reflect within a few moments to 24 hours. For any query or assistance please reach out to us @ **+1 (930) 205-4240 / +1 (930) 205-4240.**

Invoice Number –PYTU8954TY

Product	Issue Date	Expiration Date	Qty	Amount
McAfee Security 360 Plan	June, 17, 2021	June, 16, 2026	1	$398.99

PC Solution
2950 Metro Dr #104,
Bloomington, MN 55425, USA

You are important:-

In case of any dispute or query or to cancel the subscription please reach out to our support team @ toll free

+1 **(930) 205-4240/ +1 (930) 205-4240** and get a full refund. Please note you have 24 hours to report a dispute.

Thank You.

#PCSolutions_ McAfee

(1) This bulletin is intended to provide a simple and effective method to spot blatantly fake emails that use legitimate companies mixed with personal domains. However, scammer's techniques continue to evolve and as such, no method of scam detection is 100% bullet-proof.

End Elder Fraud: www.endelderfraud.org
Email: support@endelderfraud.org