How to recognize email scams!

By now I think most people are familiar with phone scams. Between telemarketers and trolls, most know what to do or better not to do.

However, I am finding a lot of people are at a loss or scared when they receive emails that sound legit but really aren't. Worse if you open up attachements that have been attached.

Recently, I have been contacted several times by people who received very real looking emails but were phishing scams. One was telling the recipient that their McAfee Anti-virus was renewed, and their Credit card was charged. Fortunately, the recipient didn't recognize the Credit card no. Still concerned they contacted me.

Another resident has someone using their email address to send emails to residents and many others. However it isn't his real email address they are using. They are using his email address as their name only so that it comes up looking like the real email address.

How can someone do that? If your email address is billybob@gmail.com. You open a new email account which might be scamyou@icloud.net but when it asks for your name you would put billybob@gmail.com

Email servers will use the name in the emails sent out to make it easier to recognize the email. However that being good also has a corrupt side like in the case of billybob@icloud.net.

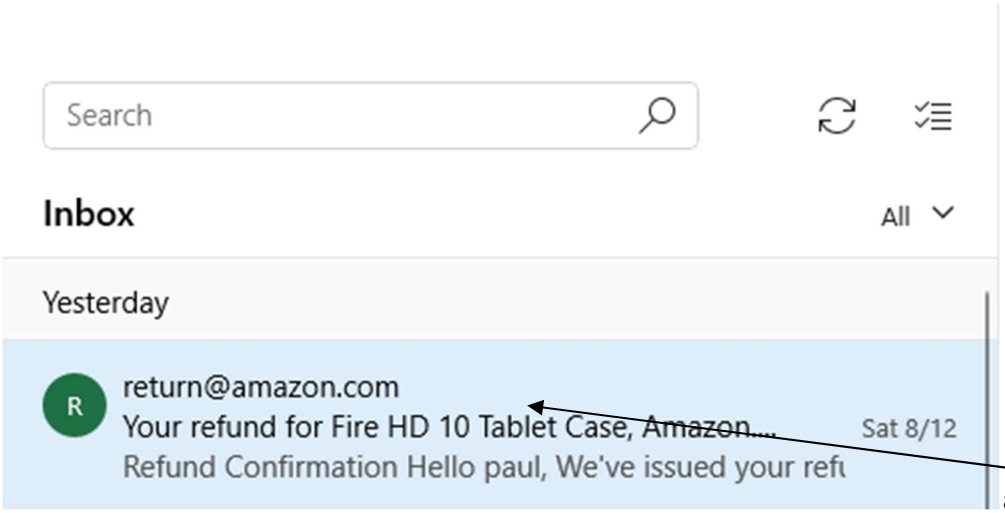
So how do you recognize bogus email!

When you get an email that seems real but the information is troubling or suspicious like billybob@gmail.com, if you were to click on the senders name like in this case billybob@gmail.com

It would then show you in brackets <scamyou@icloud.net>

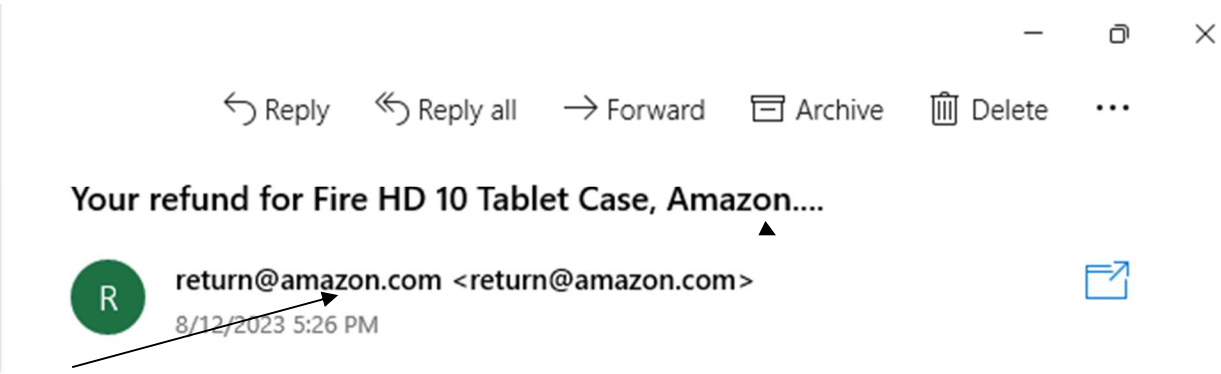
Here are some real time examples:

These 2 are legitimate emails and NOT Scams: Example 1



amazon widely used by me

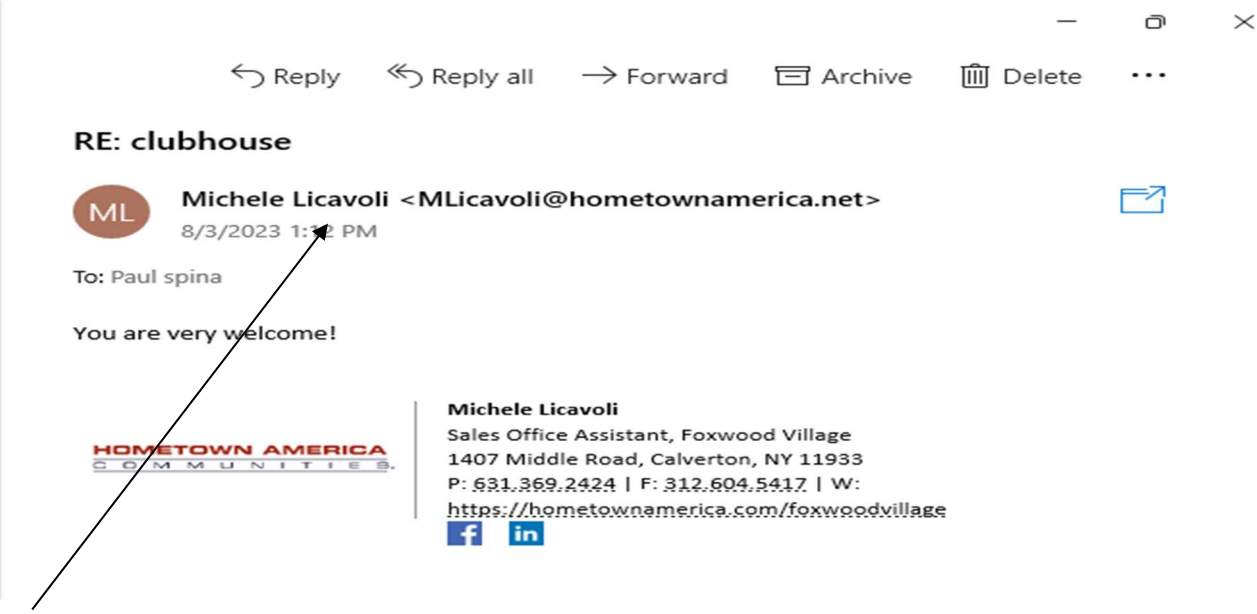
So I would be immediately drawn to the email but if I had any suspicion here is what I would do…



by clicking on return @amazon.com we yield return@amazon.com and we know it is OK

Example 2

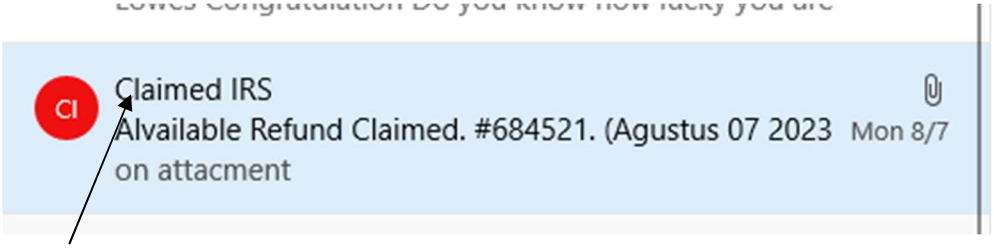
Michele works in the office here at Foxwood so it would seem legitimate.



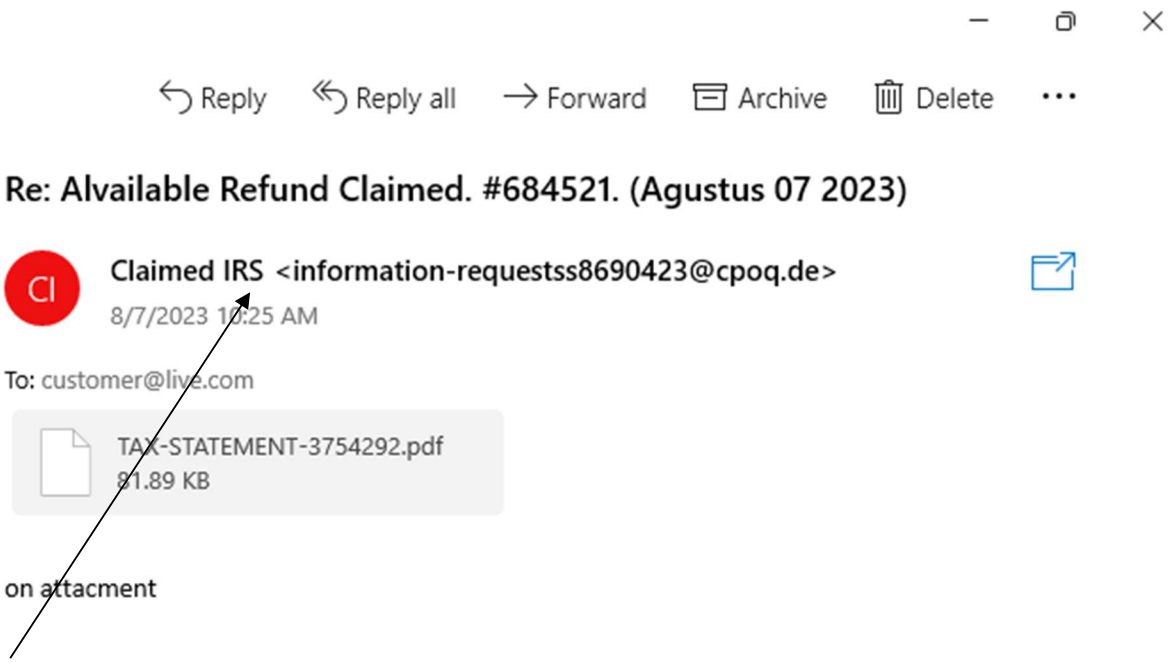
By clicking on her name we see< MLicavoli@hometownamerica.net > and we know it is OK.

Examples of Phising Scams

Example 1



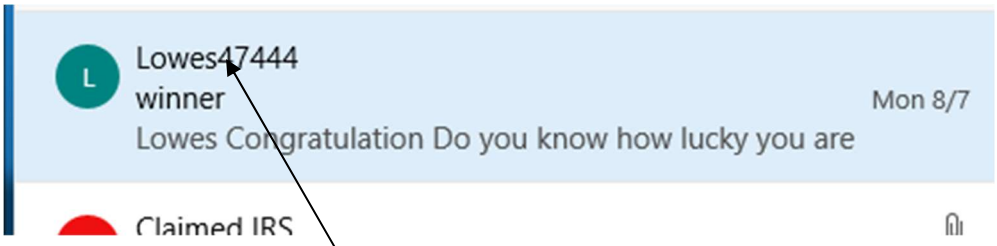
IRS we all know the IRS and receiving an email can trigger anxiety and concern even if unsuspected



In this case by clicking on IRS you get a very weird and strange email address that soesn't show IRS or .GOV. To make matters worse, you would be in real trouble opening the attachment. This email even

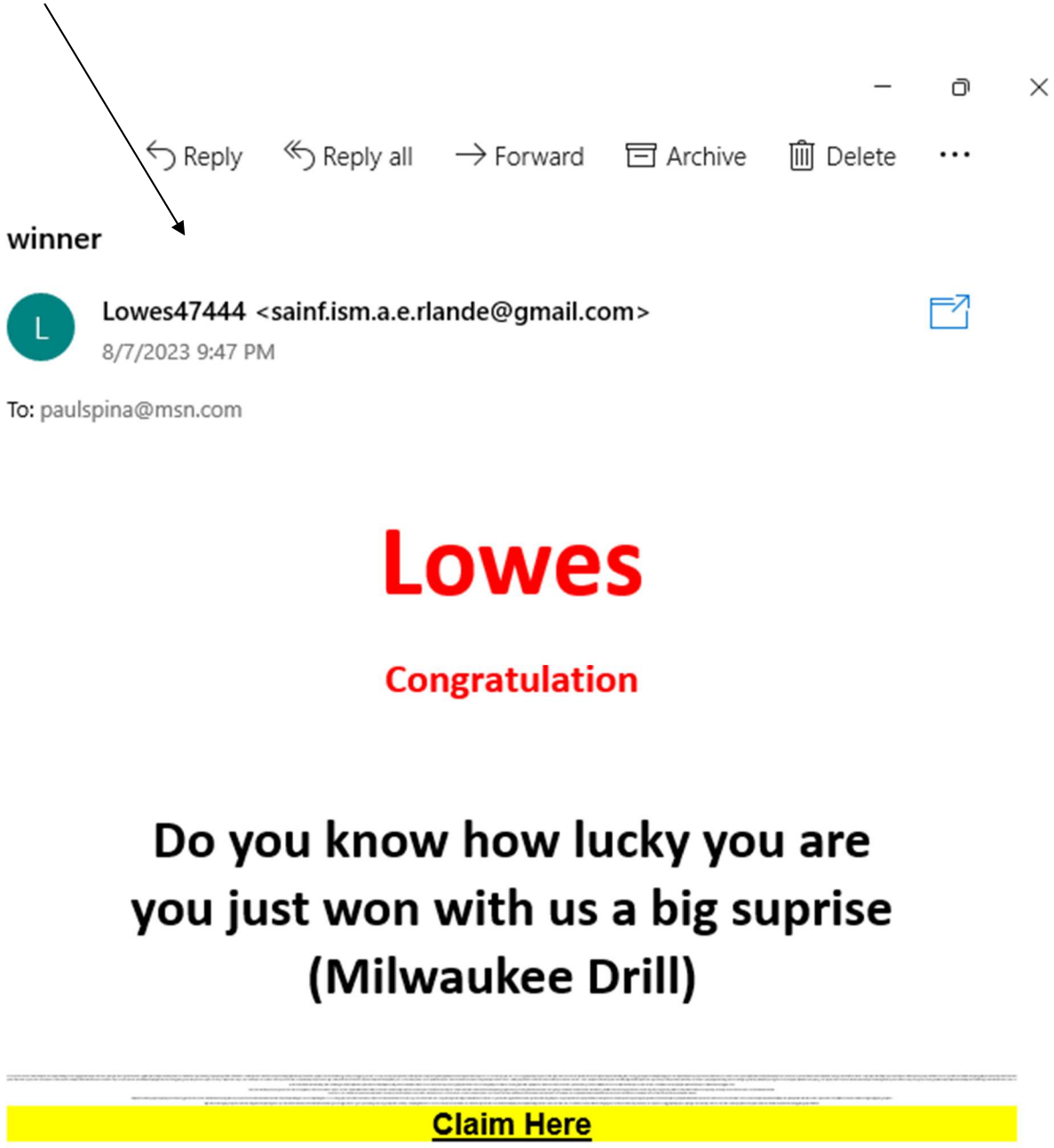
had the symbol IRS but anyone can add a picture (IRS **) like that.!!!**

Example 2



Here we have the popular store Lowes. I shop online there often. So at first glance I might open it. But I didn't order anything, and it looked a little suspect so what do I do?

I click on Lowes 47444 and reveal a very strange email address not at all from Lowes as it has no mention of the store. While I would love a Milwaukee Drill for free, I would need send them probably a credit card no. for the shipping. Then they charge thousands to my card.



I hope this little tutorial will help you avoid being scammed. REMEMBER, when in doubt DELETE THE EMAIL. If is is important, they will contact you again or some other way.

IRS, Social Security and most government agencies never email sensitive information. I'll say that again, the US Government will NEVER email sensitive information. Social Security if you have an online account with them like Medicare might email you to go online to your account and check documents but they will never email you sensitive information in the email.

The Government likes to spend our money and if you owe them money, or are being audited, you will get a Certified Letter.

Be Aware, Be Alert and Be Safe