Online Technology Safety

- Scams – Spam, Phishing, Spoofing and Pharming

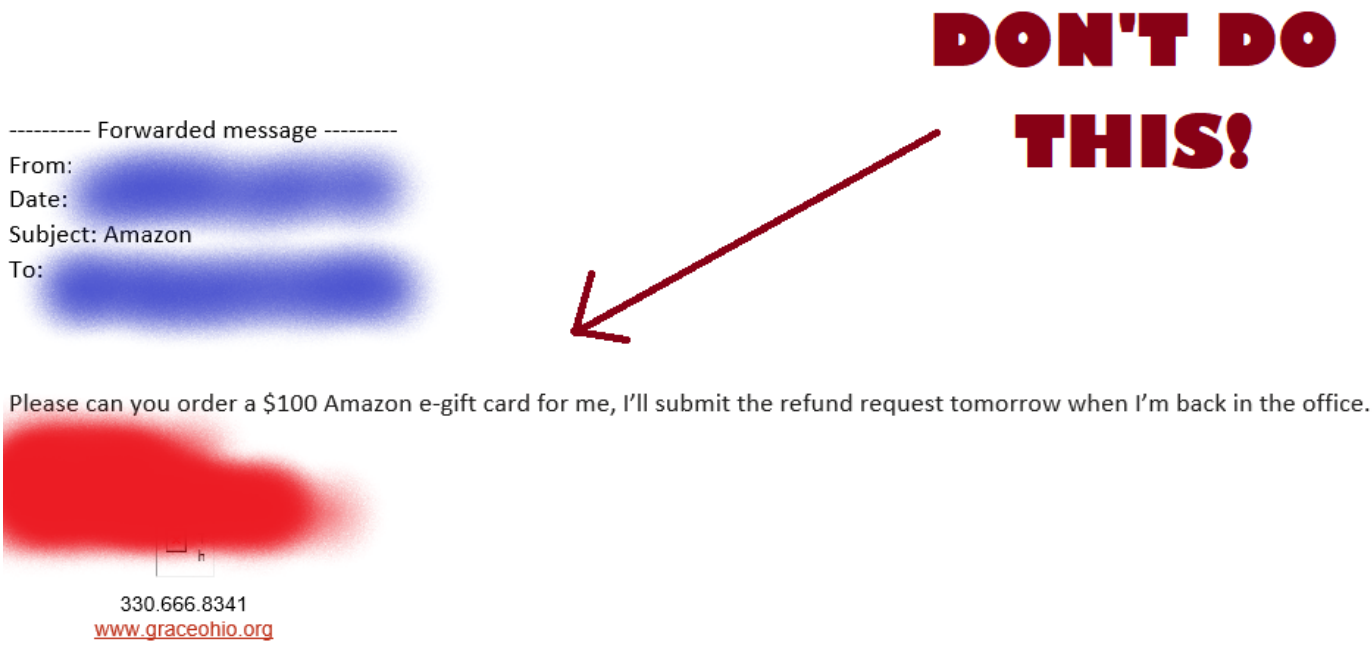
Scams – Spam, Phishing, Spoofing and Pharming

Learn more about Online Scams:

- **Scams – Spam, Phishing, Spoofing and Pharming | Be in Charge of Your Digital Life | Cybersecurity Awareness Program: Lubbock | TTU**
- **Spoofing and Phishing — FBI**

Email Safety

See it so you don't click it

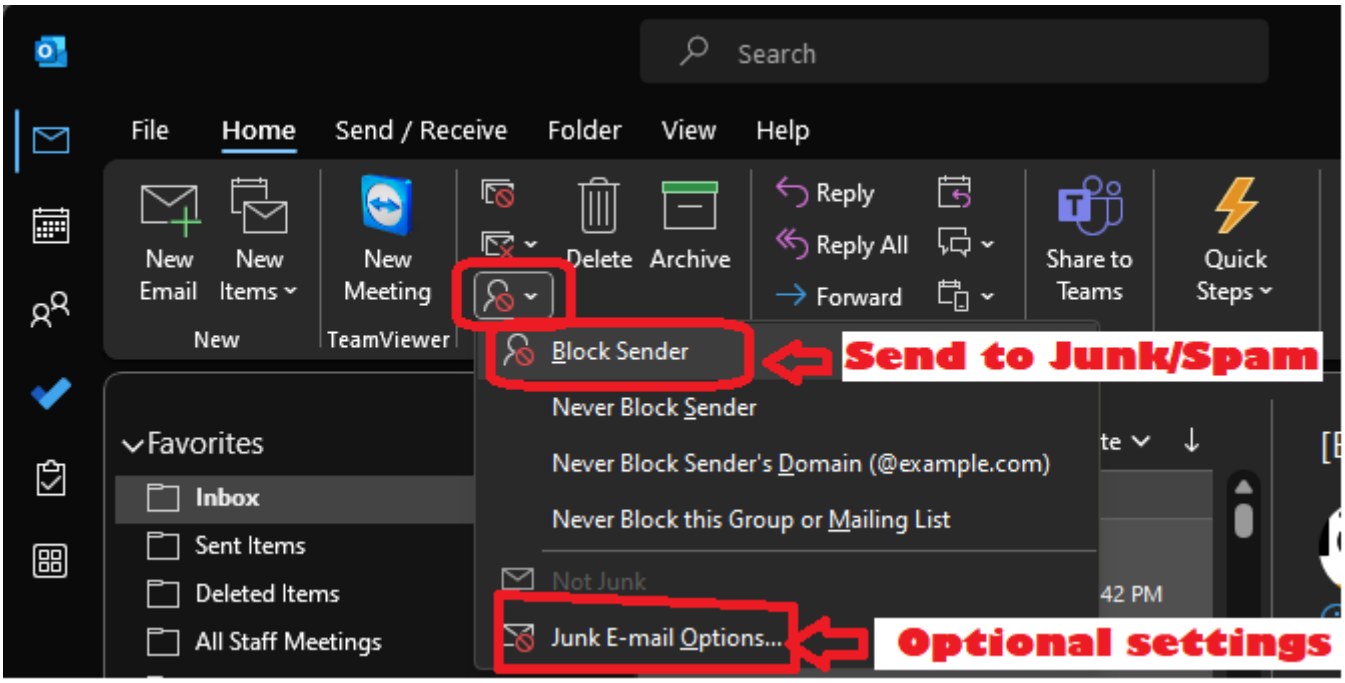


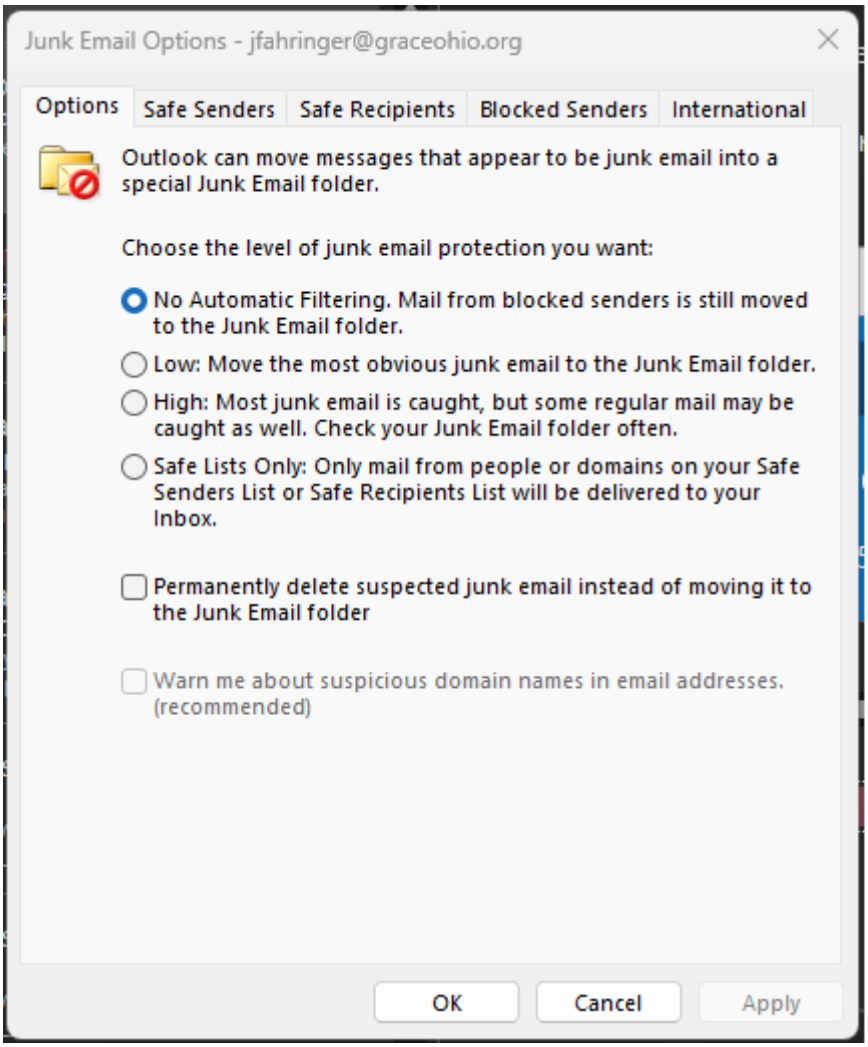
The signs can be subtle, but once you recognize a phishing attempt you can avoid falling for it. Here are some quick tips on how to clearly spot a fake phishing email:

- Contains an offer that's too good to be true
- Appears to come from a "person of interest" or someone else whom you don't normally communicate with
- Language that's urgent, alarming, or threatening
- Poorly-crafted writing with misspellings, and bad grammar

- Greetings that are ambiguous or very generic
- Requests to send personal information
- Urgency to click on an unfamiliar hyperlinks or attachment
- Strange or abrupt business requests
- Sending e-mail address doesn’t match the company it's coming from

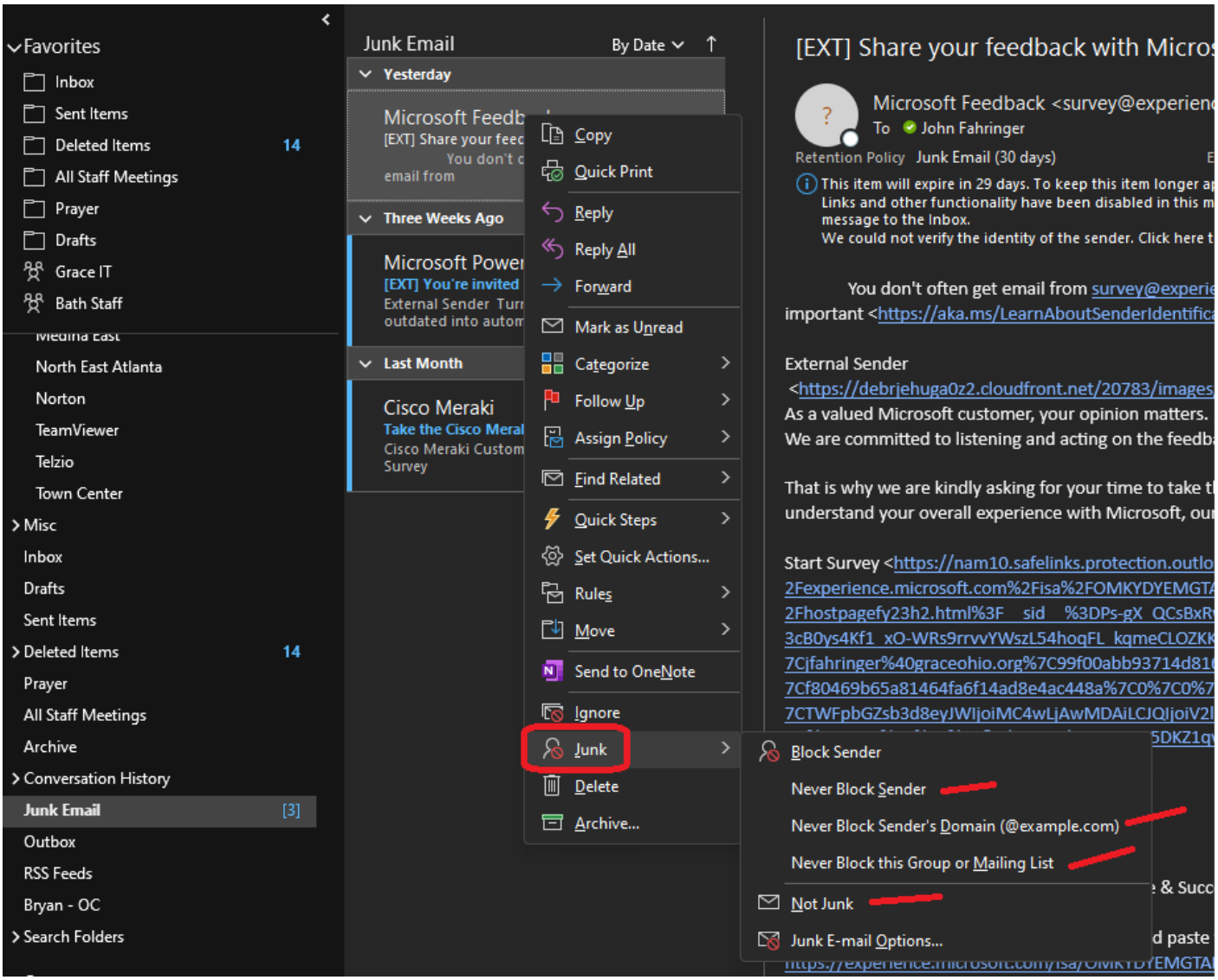
The best thing you can do to deter cybercriminals in Outlook is to utilize the Spam filter. This moves messages you deem as "unwanted" into the Spam/Junk folder, and it also reports the sender to Microsoft as a questionable sender. Future messages from the sender address will be moved in the Spam/Junk folder. With the message open, in Outlook click on the "Home" Tab, click on the Junk/Spam icon for the drop down menu, and click Block Sender. You will also see there is a choice for adjusting "Junk E-mail Options", these are additional settings that let you tweak your Junk mail preferences.





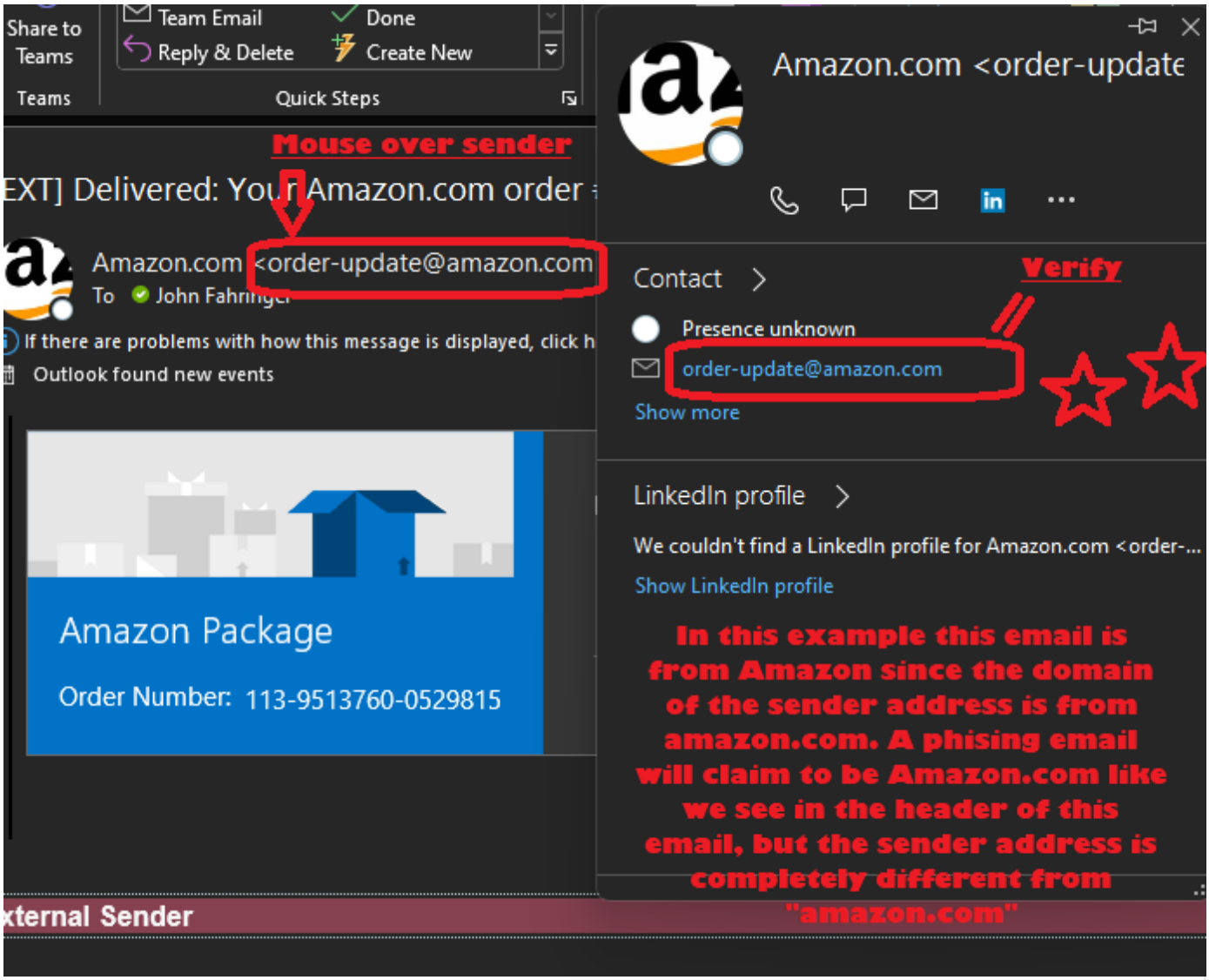
Optional Settings: Feel free to try them if you are receiving a lot of unwanted outside email. If you choose a High level of protection or something similar, you may need to keep an eye on your Spam folder for *false* spam detection (i.e. an important email being sent to junk)!

If you accidentally mark something as spam that you didn't mean to, you can navigate to your Junk Email folder and find the email you accidentally moved. Right click it, mouse to Junk, and then choose an appropriate action. For example you can unblock the sender if you blocked them by accident. Once you are satisfied with the options, you can click Not Junk to move the email out of the Junk folder.

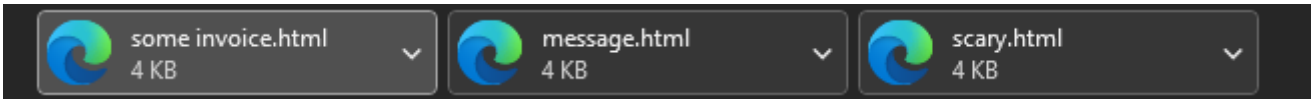


You can *always* "fact check" an email sender if you catch something unusual with the email. Do this by looking specifically at the sender address. For example, if their email address domain doesn't end in gracechurches.org, graceohio.org, or gracegeorgia.org, then the email was definitively sent from outside of our organization. Take a look at the below example of the sender address for Amazon:

Sender Address Example



NEVER EVER open any attachment in an email originating from outside that you don't recognize. This attachment is very likely designed to compromise your computer and cause very bad things to happen.
v v v



For this very reason, we don't allow ZIP files to be sent/received via email in our tenant since malware in a ZIP file can easily mask itself from antivirus scans and avoid malicious detection. If you or someone you know is trying to send several files to the other person, look into using cloud storage like OneDrive or Google Drive to share files from there. Reference our Sharing guide for OneDrive and SharePoint if you need to share several files:

Share Links with Non S... | Grace Church KB (gracechurches.org)