Is that email for real?

Whether you're still working from home or you're back at the office, protecting yourself from email scams is still important. In this article we will show you how to verify the identity of suspect email senders. Just another way TekResults is working to keep you safe.

How to verify the identity of an email

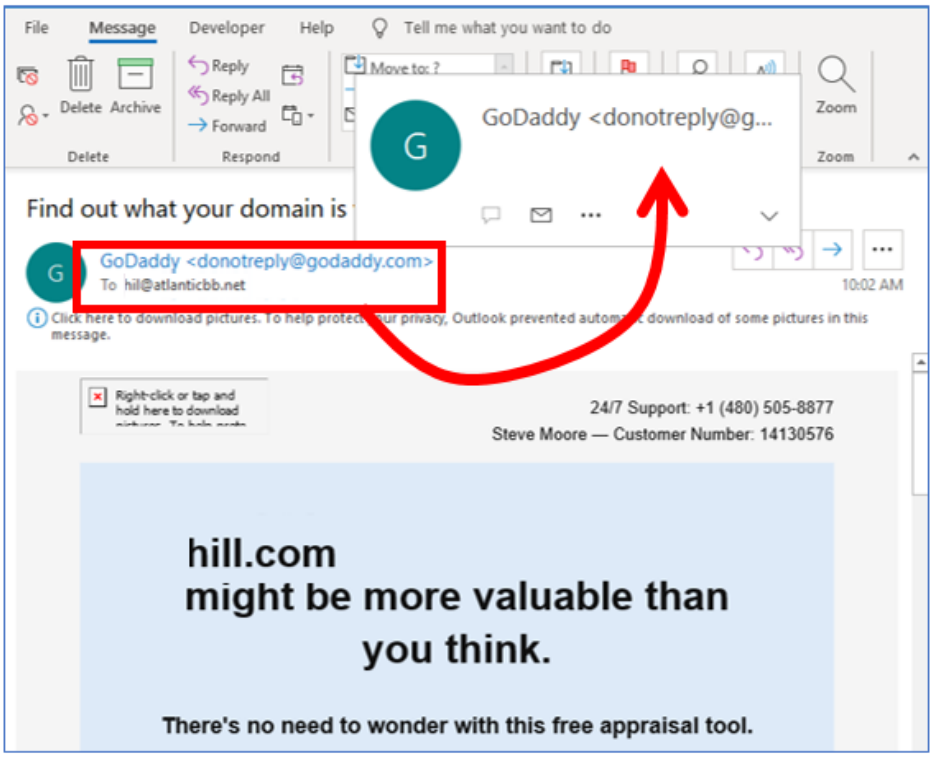
You've probably heard the term phishing -pronounced "fishing", and both spellings mean pretty much the same thing. In both cases, someone puts bait in the water and waits to see if he gets a bite. In email terms, you are the fish and some hacker, somewhere, is trying to get you to hit on his bait. Attackers use phishing emails as an easy means to acquire credentials to break into networks or to download malware in order to take control of networks or steal (or ransom!) valuable information. Usually they do this by impersonating someone you trust, like a bank or your email provider. The end result of the impersonation is to get you to enter your username and password, or some other valuable information, into a web page and make you believe you're using that information on a trusted site.

There are a few common things to look for when trying to determine the legitimacy of an email sender. Implementing these three common practices will go a long way to protect you. Since most of our clients use Microsoft Outlook as their email client our examples will use Outlook. However similar methods are available to determine if emails are legitimate for other services such as Mozilla Thunderbird, GMAIL, etc.

Verify

The easiest, and still one of the most effective, ways to protect yourself is to verify the sender.

If you are using Microsoft Outlook, first hover over the **From** display name to see what email address pops up (to hover, move your pointer over the information that you want to verify). It's very common for an attacker to spoof a display name to look like it is coming from someone legitimate, but when you hover over the display name you'll often find that message is actually coming from someone else.



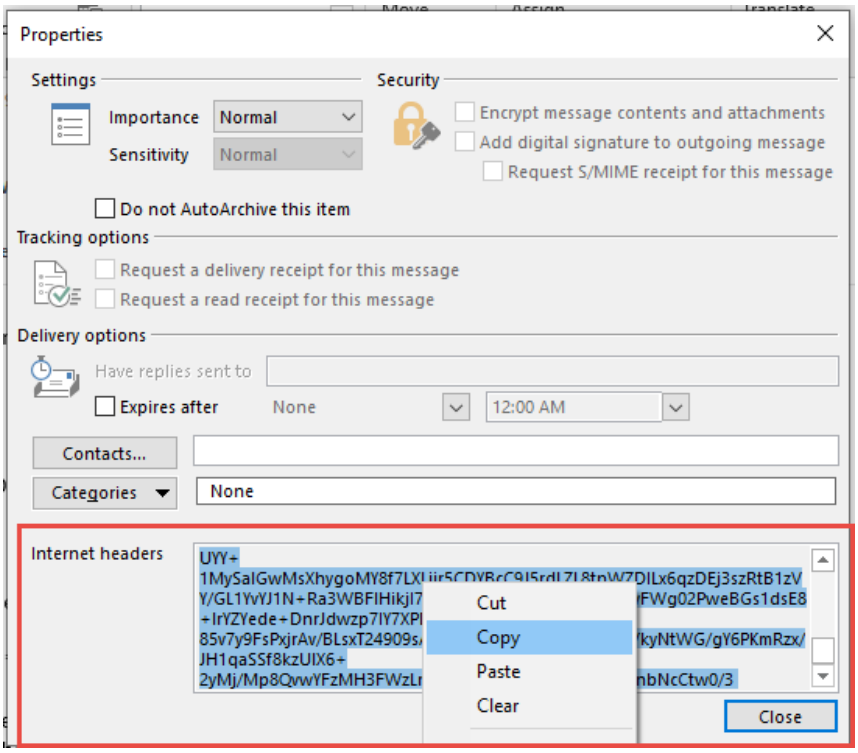
Inspect

Some attackers work a bit harder and make it a bit trickier to expose their scam. For these, you need to dig a little deeper.

Remember when we hovered? Let's go back to the email that showed up and take a closer look. Many times the attacker will employ a slight-of-hand (like magicians do) so you think you are reading an email address correctly but they've actually switched out, added or replaced characters (commonly known as substitution and transposition). It's common to see legitimate email addresses with an "m" replaced with an "rn", a lower case "L" switched out with the number "1" or a .com email reading as .co instead. Even the slightest change in an email address means the email is going somewhere else.

We always recommend checking the email header to determine where an email actually came from. Here's how:

1. Open the message in a window of its own (in Outlook, double-click the message).
2. Go to File > Properties (Properties is in the right panel).
3. Select all the text in the **Internet Headers** box and copy.



4. In a web browser go to [mxtoolbox Email Header analyzer] and paste your email header in the box.
5. Click the **Analyze Header** button.

6. The first row should tell you where the message actually originated.

Hop	Delay	From	By
1	*	MN2PR17MB3086.namprd17.prod.outlook.com	(MxWatch Service)
2	0 seconds	MN2PR17MB3086.namprd17.prod.outlook.com 10.255.180.205	MN2PR17MB3344.namprd17
3	3 seconds	MN2PR17MB3344.namprd17.prod.outlook.com	(MxWatch Service)

Search

Another great way to find out if a sender is legitimate is to do a search on the email domain on a site that is designed to assist in this detective work– this is especially useful for messages you receive from new contacts or people you aren't as familiar with.

Verify the domain name ownership and set-up details. Sites like network-tools.com and mxtoolbox.com allow you to find out details about when a domain name was set up and often who the owner of the site is. If a site was created in the last 90 days but the promising new vendor tells you that they've been in business for the past three decades, you might want to question the legitimacy of the message.

Other Clues to Watch For

In addition to trying to verify the legitimacy of the sender, there are other common clues to be on the look-out for in the body of the email, including:

- Unusual grammar or phrases: Does the email message seem a tad bit too polite for this particular co-worker? Then odds are, it's not him.
- Poorly written emails or emails that look like they were generated by a machine can also be a clue.
- Emails sent at odd times: If you are used to getting invoices from a vendor on the first of the month but get one in the middle of the month, it's worth questioning. Similarly, if you have a client who consistently emails you only from 8-5 but suddenly sends you a message in the middle of the night, it might be worth a follow-up call to verify she sent the message (and to ask why on earth she was working at midnight!).
- A sense of urgency to respond: Is the message unusually pushy, asking for immediate action (often paired with some sort of dire consequence if you don't respond)? Don't take the bait and act out of panic.
- The link in the email doesn't match the destination address: Remember that hover trick we used to verify the sender's email address? Use that to verify the links that show up in the email message are pointing to the same web address that you'll go to when you click on the link. (If you are viewing from your phone, try holding down your finger on a link to get the same pop-up.)

So how can you guarantee you don't fall for a phishing scam?

Applying these two actions consistently will help to protect you from online scams:

1. **Use your own link.** If you use the company that is the supposed sender of the email, you can bookmark the website in your favorite browser.

2. **Install or activate a web tool that identifies malicious sites for you so you know the website you find is legitimate.** There are several tools that will do this for you. Every standard browser now has a tool you can turn on to alert you if a website you are about to click on, or just clicked on, is safe or malicious.

If you find you are the victim of a phishing scam, change all your passwords immediately. If you use the same password for multiple sites (we hope you don't), cybercriminals could be in the process of trying to access other commonly used sites. Consider using a password manager in the future to lower your risk profile, and make sure you have an antivirus solution with secure web browsing features installed and up to date.

Referrals

TekResults owes much of our success to our loyal and enthusiastic clients. It's those of you who tell your friends about us that keep our company growing, and we'd like to say thanks. Just telling someone about us is all it takes. Just let us know you dropped our name and we'll drop a gift card in the mail for you to enjoy a great meal at a Dante's restaurant. See… who said talk is cheap!

The TekResults Team
support@tekresults.com
814-206-0000 Option 1

Our Services and Products

- IT problem solving
- Office 365 sales and support
- Business phone systems (Comcast, VoIPLy, Vonage, Fortinet)
- Infrastructure design and implementation
- Pre-Sales consulting
- Capacity planning/ system design
- Network cabling
- Security compliance review HIPAA
- Security compliance review PCI
- System installations
- System upgrades
- System auditing / documentation
- Desktop, laptop and monitor and other sales
- Network administration
- Network troubleshooting
- Business consulting software testing and service
- 3rd party software setup and support
- Computer security solutions (including PGP, encrypted mail, secured transactions)
- Custom application development
- Legacy system migration and rewrites
- System integration
- Application integration
- Network installation and integration
- Training and staff development