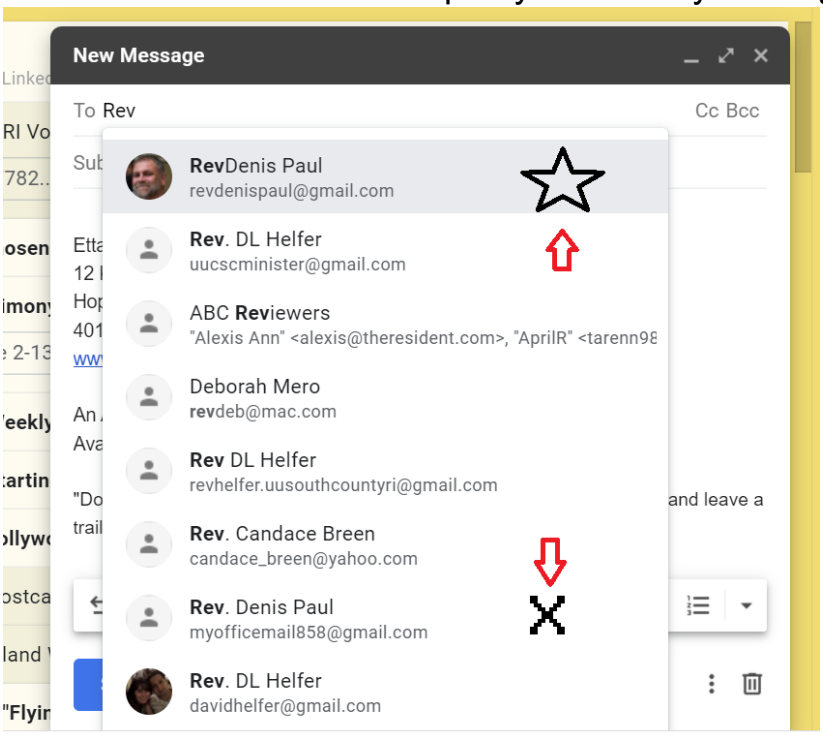
Understanding Phishing: The first step in protecting yourself from fraud

Phishing emails are created explicitly by hackers to try and convince you to give up pertinent information or your hard-earned money, seemingly for a good cause.

They look legitimate at first, coming most likely from a source you trust – your bank, credit card, a good friend, and very commonly your minister! Always hover your mouse pointer over the sender to verify that the sender's email is one that you recognize. Just for the record, Rev Denis' official email is: revdenispaul@gmail.com. Any variation from that official one is a hook. Don't bite! Don't click or open anything. Just delete the email and move on.

Be aware that email programs may automatically save all incoming email addresses and offer them up to you for easy clicking when you are composing a message. Choose the correct address here, and then open your Contacts, search for Rev Denis and delete the incorrect address there.



Deleting a phishing email address in your contact list will lessen the chance that you might send a message to the wrong email address to be lost in cyberspace, leaving you wondering why you are getting no response. Also, sending any emails

to the fake address can also confirm to scammers that you are a “live” mark, and open for further scams. Not what you want to do!

The latest wave of phishing scams has shown up on social media sites like Facebook, Twitter, and Instagram. Direct links to spoof websites are created and proposed in a way to look legitimate, so users click on these links and believe they are being routed to legitimate websites. Fun quizzes, enticing sweepstakes, and stupid challenges are clever ways that phishermen/women gather private information on you to use for nefarious purposes.

Here are some general tips to remember to protect yourself from fraud:

Red Flags to Look For

- Any request for you to buy gift cards or send money to the caller.
- Any request for you to send a new transaction such as payment reversal.
- Request to install any software or apps on your device, especially remote desktop software. This software risks giving the caller the ability to control your device.
- Request for you to login to any of your banking, shopping, or investment accounts while on the phone or screen sharing.
- Request for you to provide your personal information, user credentials, or account information.
- Any claim that an error has occurred, and the caller or you are in trouble if it is not corrected.
- If the caller is pushy, aggressive, raises their voice, is rude, or gets angry.
- Any claim that there is a virus on your computer, and you need to fix it immediately, either by clicking a link or by giving a phone caller access to your computer.

How to Protect Yourself

1. Only call trusted phone numbers associated with your bank or merchant in response to a question or concern. You can find this readily on the company's website or the back of your credit or debit card.
2. Before calling a number or clicking on a link in an email or text, login to the account in question and see if there has been any transaction that you don't recognize or any alerts or notices to your account. **Never login to an unknown link.**
3. If you have been targeted or fallen victim to a scam in the past, unfortunately you are likely to be targeted again. So, be even more skeptical when you receive that call, email, or text.
4. When making purchases online, be cautious of deals that seem too good to be true.
5. Anyone can set up a shop or post an ad on social media. If you can, try to have a video call or in-person meeting with the seller to meet them and see what you are buying — especially if it's a big-ticket item like a used car or pet.
6. Before sending money, do an online search of the company, seller, or service. Keep in mind that if there are either no reviews, or all good reviews, these can be red flags, too.

The latest nuanced scams to watch for:

Refund Fraud:

- The scammer tries to convince you that there was a billing error, they are verifying a recent transaction, or that you are owed a refund related to a purchase.
- They offer to help fix the issue by having you install a remote desktop software or app on your device.
- The real purpose: to trick the customer into believing that once the "refund" has been processed the customer will receive significantly more than entitled to receive.
- This induces panic for the customer by indicating that "the customer service rep" will be fired due to the error – or the customer will be in legal trouble if the funds are not returned.

Reversal Fraud:

- The customer receives a fake text alert for a suspicious electronic or cash app transaction.
- Once the customer replies, they receive a call with an offer to fix this by initiating a “payment reversal” transaction.

Etta Zasloff with excerpts from:
https://doingmoretoday.com/7-red-flags-to-help-you-avoid-fraud/