Is this email fake? How to avoid phishing scams

By Jeremy Steele

Jeremy Steele *is the associate pastor at Los Altos UMC in Los Altos, California, as well as a writer and speaker. You can find a list of all his books, articles and resources for churches, including his most recent book All the Best Questions, at his website: JeremyWords.com.*

A couple years ago I sat down at my desk, fired up my computer, and saw an email from the senior pastor at the top of my email inbox with the subject "Hello." That was not his typical subject line, but I opened the email and read, "How are you? I need a favor from you, please email me back as soon as possible. Hope to hear from you soon."

It was fake, and it was the closest I've ever come to falling for what is known as a phishing email. What is phishing? Phishing emails are when a scammer impersonates some person or organization in hopes of getting the user to reply or click a link. When done well, these emails play on our automatic trust and reflex to reply. They are common and often use current issues to their advantage. Last year Google saw 18 million daily malware and phishing emails just related to COVID-19.

They aren't all as simple as the pastor email example. Some emails appear to come from your bank and redirect you to a page created to resemble your bank's login page. Once you put your username and password in, even if you don't hit submit, the scammer has what they need to log in as you and do real damage.

How do you avoid falling prey to phishing scams? Try these five simple habits that can help you protect yourself against this tricky tactic.

1. Trust your instinct

If something feels off, assume it is. There are a number of things that can tip you off that something is not right:

- You don't have an account with the business that contacted you
- Grammar errors and/or misspellings are present in the email
- There is a direct ask for money
- They ask you to confirm personal information
- An unexpected invoice is attached
- They want you to click on a link to make a payment or log into your account
- You are addressed by the sender in an unusual way like "Hi dear" from your bank or "Sir" from your relative

Small things may feel off, but we may overlook them because they appear to come from a person or organization we trust. When something feels wrong: Pause. Don't click. Don't reply.

2. Check the email address

When you aren't sure about an email, first check the sender's email address. Though it may look like a legitimate address, email apps on phones and computers can mask the real address. To reveal a possible hidden address, with your mouse hover over the sender's email appearing in the "From" field. A bubble showing the sender's true address will appear. Instead of hovering you can also double click on the address in the "From" field to see the underlying sender.

You'll often notice it is not your friend's address or from the real company's domain. Instead of @yourbank.com, it may be from a yahoo or gmail account. If that is the case, mark it as spam, delete it and forward it to the federal trade commission's anti-phishing working group: reportphishing@apwg.org.

3. Go to the correct source

Advanced hackers are able to mask email addresses so that the right address actually appears in the "From" field. If something seems suspicious about the email but the address appears valid, the next step is to go to the correct source of the email to verify the claims. If it's your friend, a call or text asking if it is legit is in order. If it's your bank, visit their website by typing it into the address bar of your web browser, log in and see if there are any notifications or if anything seems to be a problem. You can also call the company or find their customer service email address on their website to verify the message you received was legitimate.

4. Enable two factor authentication

Most accounts allow (and many require) you to enable two-factor authentication. When enabled, it requires you to prove you are who you say you are using two methods (like a password and a text message verification) instead of just a password. Though it doesn't deal with your phishing email directly, enabling two factor authentication means that even if someone is able to trick you into giving your password, they won't be able to gain access to your account without also having your cellphone or other second factor device.

5. Check the url

If you still feel the need to click the link in the email, there are several services that can help you check it before you click away. Some urls are "shortened" by using a service like bit.ly that give you an easy to type and remember url to replace the long, complicated urls generated by most websites. There are several tools like checkshorturl.com to know whether or not the shortened link is taking you where it claims. Copy the link in the email making sure not to click to activate it. Then paste it into the form and the link verifying app checkshorturl.com will let you see where it will ultimately take you. If the url doesn't appear to be shortened, but you still aren't sure, you can use Google's safe browsing site status to check whether or not the link in the email takes you to a site that has malware or other dangerous code.

Phishing emails are dangerous but avoidable. By enacting new habits and protections, you can feel confident that you are protected from this common and malicious threat.