Tech Coach Corner — Phishing

By LTCL Librarian Karen Scott

If you have ever received an email asking for payment or sensitive information that seems to come out of nowhere, you might have been a victim of a phishing attempt. Phishing emails often come under the guise of invoices, password resets, emergency asks to update information, or requests for money from someone you don't know. Simply put, phishing is a method of scamming used to gather information under the guide of a legitimate message.

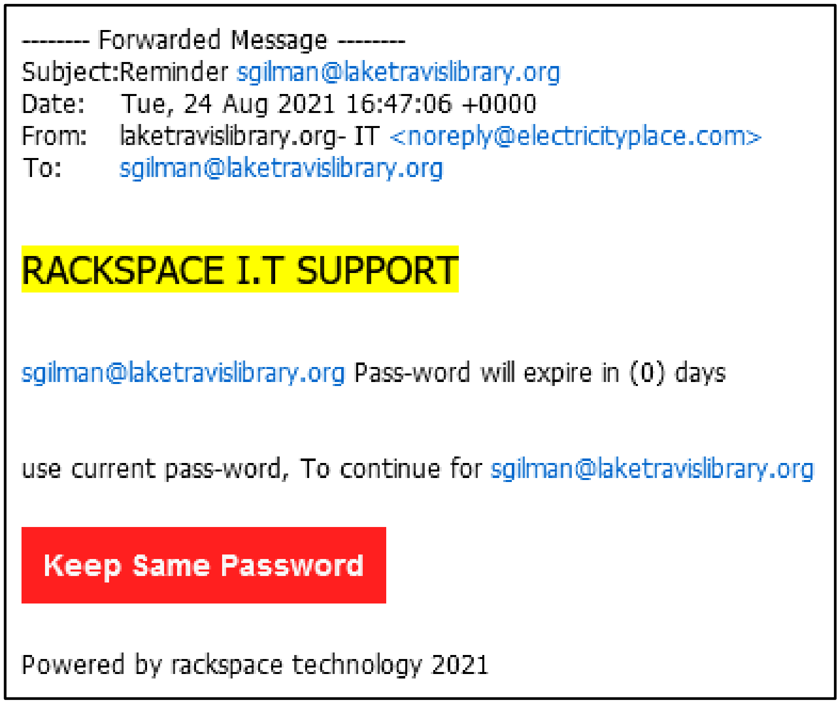
Now that mobile devices are commonly used to send messages *and* access the internet a lot of text messages are used for receiving notifications, receiving login codes, and signing up for services. Because of this new form of communication, the tiny computers in your pocket might receive a phishing attempt in the form of a text message. For example, you may get a text that you didn't request asking you to "click this link to reset your password" for a website you supposedly use. If you receive a text that you didn't ask for, delete the message immediately and do not click on any links! This is a common type of phishing.

If you're not sure whether a message is a phishing attempt or not, you should check the following:

- Sender — Does the sender's email or phone number look suspicious? Make sure to check the actual email address and not just the "name" of the sender.
- Links — Hover over the link with your mouse to see the true location; this might show up as a small preview where your cursor is or at the bottom of your browser window. On a smartphone, tap and hold on a mobile so the preview shows up.
- Attachments — Unexpected emails with attachments are a red flag--do not download anything you're not expecting.
- Emotion — Be aware that some scammers will try to use emotion to get you to send money or personal information.
- Data — Legitimate companies don't ask for information over email. If you're still unsure about an email or text that looks like it is from a company you recognize, it is best to go to their website or customer service directly rather than respond to the message.

For example, there are a handful of signs that the email below is phishing, even though it's made to look like it's coming from a trusted email service provider. First, the actual email address @electricityplace.com does not reflect the Rackspace service it is imitating. Second, there are a number of questionable grammar choices, such as "I.T" and "pass-word;" proper technology services would not use this style. The last line including "rackspace technology 2021" in all lowercase letters also does not reflect professional IT operations.

If you're unsure about whether an email like this is legitimate you should visit the provider's website directly and change your password if needed.



-------- Forwarded Message --------
Subject:Reminder sgilman@laketravislibrary.org
Date: Tue, 24 Aug 2021 16:47:06 +0000
From: laketravislibrary.org- IT <noreply@electricityplace.com>
To: sgilman@laketravislibrary.org

RACKSPACE I.T SUPPORT

sgilman@laketravislibrary.org Pass-word will expire in (0) days

use current pass-word, To continue for sgilman@laketravislibrary.org

Powered by rackspace technology 2021

Stay safe!

Tech Coach Assistance

Tech Coaches are now providing remote Tech Coaching. Simply send an email to techcoach@laketravislibrary.org and one of our coaches will respond to assist you with any questions or challenges you may have.