TECHNICAL UPDATE

CTSI Serving Colorado's Counties

Volume 26 Number 8 February 22, 2022

How to Identify a Phishing Email

Phishing emails are malicious emails that ask the reader to click on a link that will install harmful software on the receiver's computer and network; they can look almost identical to legitimate emails. Cybercriminals will often take the time to copy logos from legitimate companies and even mimic the text of an email. The best way to avoid a phishing scam is to hover the mouse over the link you are asked to click on and view the web address. If the web address does not contain the company name or looks suspicious in any way, do not click on the link.

WHY DID YOU RECEIVE THE EMAIL?

Another step you can take to identify phishing emails is to consider why you received the email in the first place. Most companies send confirmation emails only if you signed up for a new service or made a change to your account, such as updating information. If you did nothing to trigger such an email, be suspicious. Also, be wary of emails that do not fully load or display correctly. Many companies bundle plain-text and HTML versions of emails together to ensure that they display correctly on multiple email clients; cybercriminals often do not bother with this step, so their emails may display with missing graphics or text.

Cybercriminals can steal email signatures from people you know and with whom you regularly do business. If you receive an email with an attachment, a request to divulge information, make a money transfer, buy something, or pay an invoice, even from someone you know, approach it with suspicion and then look for reasons to trust it. Never allow an email attachment to "Enable macros" in Microsoft Office. If you open a PDF that wants you to log in to Microsoft, don't do it. A PDF has nothing to do with Microsoft 365. If you're curious why the individual is asking you to do something or if they sent you something you weren't expecting, pick up the phone and call them.

HOW IS THE EMAIL WORDED?

Phishing emails are often sent to large groups of people in the hopes of tricking a handful of recipients into taking the bait, so look out for generic subject lines and greetings. The text of the email is often vaguely threatening or alarmist, stating that if you do not click on the offered link or enter your personal information, your account will be closed or your data compromised. Legitimate emails will never ask you for your personal information or password. Any organization you are a member of already has this information.

WHAT THIS MEANS FOR COUNTIES

CTSI does provide coverage for cyberattacks, as discussed in Technical Update vol. 23 no. 10 parts I and II; however, the best way to protect your organization from cybercrime is to be diligent and proactive. Trust your instincts. If something about an email seems off (e.g., an unusual request, odd URL, etc.), be suspicious. Do not click on attachments or links if there is any doubt about the validity of an email, even if the sender is someone you know. Contact the sender and ask if they sent you the email. For questions about recognizing and avoiding cybercrime, contact CTSI at (303) 861 0507.