Cybersecurity
TIPS & TRICKS

Malware Can Live in Email Attachments

Email attachments, including links, PDFs, and Word documents, may contain malware (viruses and other code that can infect your computer systems). Cyber criminals are very good at disguising attachments that contain malware in attachments that look very much like FedEx/UPS delivery tracking notices and credit card, bank, or USPS notifications.

While we can't prevent the intrusion of all malware, a little healthy skepticism can prevent a lot of harm. When you receive an email with an attachment ask yourself the following questions:

1. Did I expect this attachment?
2. Do I know the sender?
    a. Hover the cursor over the sender's email address and check that it matches prior emails you have received from that person.
    b. If you know the sender you can send him or her a text message (don't use the same email address in "Reply" that contains the suspicious attachment) or call and ask if they sent this to you.
3. If you don't know the sender, or if you do but weren't expecting the attachment and can't reach the sender to confirm it's legitimate, do NOT click on it. Forward it to your IT team to scan for malware and don't open it until you receive a "safe to open" message back.

This Cyber Tip was brought to you by the Cyber Security Subcommittee of the Primerus Quality Assurance Board and featured contributor Kenneth Rashbaum of Barton LLP. We welcome your tips, which can be submitted to Paige Neirman at pneirman@primerus.com for publication consideration.