What should I do if I suspect a Phishing Attack?

Jamshid Javidi, CEO Computers

Answer: As of late, this has been a question we have received on an almost weekly basis. Phishing attacks are becoming incredibly sophisticated and harder to detect. More and more hackers nowadays are doing surveillance work before sending a phishing email, creating much confusion on the user's end when it is received. They may monitor your emails for a while and gain access to private information such as your work title and position at the company. They may also know who your boss or coworkers are and your work relationship. For example, they may know who is in accounting and pays the invoices, who are your vendors, and much more. Sometimes they even create a website and emails very similar to yours with a minor difference that is not easy to catch. For example, mary@Dominion.com looks very similar to mary@Dominon.com. So, it pays to be super careful with a suspicious email.

Troubleshoot the situation

If you get an email or a text message that asks you to click on a link or open an attachment, answer these questions first:

- Was I expecting this email? If the answer is "*No*," it could be a phishing scam.
- Do I have an account with the company or know the sender that contacted me? If the answer is "*Yes*," contact the company or the sender using a phone number or website you know is real. Not the information in the email. Attachments and links can install harmful malware.

To detect the email's authenticity, hover over the sender's email (without clicking on it); this way, you will see the actual email. If it ends with letters from a country like ".jp" for Japan and others, then it is a phishing email. You will also want to adhere to the following tips to determine if you're experiencing a Phishing attack.

1. Look for typos and grammar mistakes. This is a very telling clue as the scammer uses typos to fool the algorithm into thinking they are new words, thus bypassing spam filters and allowing the emails to make it into your inbox.
2. If there is an urgency and telling you to take action now (your password had expired, the account is on hold because of a billing problem. etc.)
3. Check the rules in your Outlook to see if your emails are being forwarded to another email account or a rule that you did not set.
4. In the Control Panel, look at your installed programs and see if anything was recently installed.
5. Run recent software updates. Also, Scan your computer with the latest Antivirus and anti-malware software.
6. Delete the email by holding the shift and the "delete" key. This way, the email is completely deleted from your inbox.
7. Have cybersecurity awareness training for your staff.

What to Do If You Responded to a Phishing Email?

If you think a scammer has your information, like your Social Security number, credit card, or bank account number, go to IdentityTheft.gov. There you'll see the specific steps to take based on the information that you lost. Call the banks and other institutions and tell them what happened. Change passwords immediately.

- If you think you clicked on a link or opened an attachment that downloaded harmful software, turn off your computer immediately, contact us or contact your IT company.

If you should have additional questions pertaining to Phishing scams, please feel free to call us at 818-501-2281 and we'd be happy to answer any questions tech related.
In the meantime, if you have a question you'd like to have answered in a future issue of ***"Tech Tip Tuesday"***, email us at **info@ceocomputers.com**.