Tips to help small business owners avoid phishing scam

December 4 2019, by Joyce M. Rosenberg

Credit: CC0 Public Domain

Phishing scams that infect a computer and potentially allow hackers to invade bank and other accounts are highly preventable—but it takes eternal vigilance on the part of computer users.

Even small business owners or employees who think they're careful about clicking on links and attachments in emails—the tools phishing scammers use—can be tricked and find their computers have been invaded. They may also have given cyberthieves access to bank and other accounts. Cybercriminals have become increasingly crafty and sophisticated with emails that look realistic.

Owners need to educate and keep reminding staffers about the dangers of clicking on the wrong things.

Some tips to avoid getting caught in a phishing scam:

— Be wary of any link or attachment. Unless it's absolutely clear from the context of an email that the link or attachment is OK—for example, your attorney has sent you the sales contract you expected in a Microsoft word document, or a staffer writes, "here's the link to the website we discussed at our meeting this morning"—assume that clicking could get you in trouble. Be particularly suspicious of emails about package shipments, invoices or that ask for personal information, logins and passwords. An unexpected email from the IRS is a scam; the agency does not initiate contact with a taxpayer via email, phone calls, texts or social media.

— Check the email address. Even if the email comes from someone you know, double-check the address it's from. Cybercriminals can take an email and make subtle changes—for example, replacing a "m" with an "r" and an "n" that you might not notice unless you look closely at it.

— Confirm with the sender that they sent you a legitimate email. If you get an unexpected email with a document or a link, check with the sender. But don't click on "reply" or copy the email address—call or send a separate email, using an address you know is correct.

— Consider restricting staffers' use of personal email browsers on work PCs. A staffer who clicks on a link or attachment in a personal email can infect the company machine or system. If staffers can't read their own email, it can reduce a company's vulnerability.