Consumer Corner with Anita Wilson: Beware when lures aren’t pretty and fishing is phishing

By ANITA WILSON
Published: 5/18/2022 1:33:28 PM

Editor’s note: In this new monthly column, the leader of consumer protection at the Northwestern district attorney’s office will focus on important consumer issues, fraud trends or other such topics.

My email inbox has been bursting at the seams lately and I bet yours has too. Every day, I have dozens of emails from senders I don’t recognize and a handful from people that I do recognize. I delete emails I know are fraudulent or offering something I don’t want or need, but some of them seem to come from companies that look familiar. “Seem to” is an important distinction: These senders are hoping to fool me by using a “phishing” scam.

Phishing sounds like the sport of fishing, but instead of using a pole and bait, these people use email to lure potential victims to take advantage — even steal — from them. They send an email purportedly from a bank, credit card company, a retailer, a delivery company, a utility, or even a government agency such as the Social Security Administration. The scammer tells you there is a problem in order to get you to bite, and once you do, they reel you in.

The email might describe one of these scenarios:

■A problem with your bank or credit card account, asking you to click on the link or call a number to straighten it out.

■A suspicious activity with your Amazon or PayPal account, with instructions to click on the link in the email to fix it.

■A package being delivered, but you need to verify your delivery information.

■Your utility bill is overdue and you need to confirm your account information and make a payment or your service will be shut off immediately.

■Your computer anti-virus software is about to expire so you need to click on a link and enter credit card information to renew.

Do you see a pattern? The sender of such emails most likely uses a link or phone number that looks real in order to get you to share your personal information, account numbers, or passwords. They can then use this information to open accounts, make purchases, and commit fraud by assuming your identity.

They all sound urgent. But don't panic or fall for this scam. Before you do anything, verify the information you see in the email — I'll explain how a bit later in this column — because even if email looks real, you cannot always trust the links or phone numbers.

Often, there are clues when emails are fraudulent. Among the red flags: Misspelled words, poor grammar, strange email addresses, a generic greeting such "Hello" or "Dear customer" or links to click on.

Phishing emails can be made to look quite legitimate. It is easy for people to copy company logos, create lookalike phone numbers and realistic email addresses to use them for nefarious reasons. That's why I suggest you use caution when opening emails and go straight to the source to check any supposed problems with your accounts. Don't provide any personal and financial information in response to an email.

If you are worried about your bank account based on an email by all means look into it, but don't reply to that email. Instead, get out your debit card, credit card, or paper statement and call that phone number or visit your local bank branch to find out if there is a problem.

If you are warned about your Amazon or PayPal accounts, exit the email and log into your account to see if there really is any suspicious activity. If you've been told you have a delivery, look up the delivery company's number and call to verify the tracking number.

If someone tells you your gas or electric will be cut off because you owe money, find your latest utility bill and call the phone number listed to check the status of your account.

And if someone you don't know is telling you to download anti-virus protection, first run your computer's security or anti-virus program to make sure it is up to date. Chances are that you will find there is no problem at all.

These scams are not limited to emails. Be wary of text messages with similar scenarios. Verify before you text back or click on any links.

Report phishing emails to your email provider by marking it as spam or moving it to the junk mail folder. Phishing emails can also be forwarded to The Federal Trade Commission at spam@uce.gov.

If you get a suspicious text, you can click on the info link (that's an i with a circle around it on an iPhone or the three dots on the top right of the screen on an Android,) scroll down, and click on the option to block that contact.

And, if you have questions about phishing or other scams, feel free to contact our Greenfield office at 413-774-3186 or Northampton office at 413-586-9225.

Anita Wilson is the director of the Northwestern District Attorney's Office Consumer Protection Unit, which is a Local Consumer Program working in cooperation with the Office of the Massachusetts Attorney General.