Beware of Phishers during COVID-19

hooker & holcombe

Yes, it's true! Our society is becoming even more technology-driven, and it is happening at a rapid pace during uncertain times as many transition to work from home environments. However, at the same time there has been an increase in the registration of websites relating to COVID-19. Experts suspect many of these new websites are the work of cybercriminals looking to exploit the spread of COVID-19 by conducting campaigns in the form of phishing scams.

How does Phishing work?

The newest technology-driven email phishing scams attempt to get your personal information (i.e., your social security number, credit card information, date of birth, etc.). The email attacks are based around emails that look like they come from a reputable business that you know, possibly a bank or charity. The email contains links or attachments that claim to contain important information about the COVID-19 virus. Once you click on the link or open the attachment, it infects the computer with malware that can be used to exploit the infected victim.

However, traditional phishing scams are still making the rounds. In this instance, the phisher would make requests such as asking you to send money to them that might be out of the ordinary, or to open an odd attachment with a vague message possibly focused around important virus information that is urgent for you to know. They would provide a phone number that you can call or offer you forms to complete to protect you – both of which are fake.

Phishers use a time of crisis to take advantage of people who may make unclear decisions in a time of fear.

Remember, phishers are focused on:

- Getting you to open attachments;
- Getting you to log on to a fake site;
- Using words such as "urgent", "immediately", or "critical" to bypass your natural instinct to review things objectively.

If you receive an odd request:

1. **Do NOT reply to the email.** If it is a request to send money or divulge some other confidential information, contact the sender by telephone at a number that is not provided in the email.
2. **Do not open the attachment.**
3. **Do not fill out forms or provide any information.**

Helpful tips to spot and deal with phishing emails:

If you haven't clicked any links in the email, that's good. Until you're certain that the sender is genuine, you should not follow any links, or reply. The next thing to do is try and identify whether the email is a scam, or genuine.

- Many phishing emails have poor grammar, punctuation and spelling.
- Is the design and overall quality what would you'd expect from the organization the email is supposed to come from?

- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is. It is pretty unlikely that someone will want to give you money, or give you access to a secret part of the Internet.
- Your bank, or any other official source, should never ask you to supply personal information from an email. Try to check any claims made in the email through some other channel. For example, by calling your bank to see if they actually sent you an email or doing a quick Google search on some of the wording used in the email.

These are tenuous times, and unfortunately, criminals try to take advantage of people when they are in distress or feel uncertain. Now, more than ever, be diligent about safeguarding your personal information.