CATIC

COVID-19 Phishing Emails: Common Scams That You Should Know About

Over the course of 18 or so months, the COVID-19 pandemic has continuously proven to be a difficult and problematic entity we are forced to deal with. Along with this new and challenging way of life that we are becoming acclimated to, there has been a troubling rise in phishing emails related to COVID-19. As one may recall, back in April of 2020 we discussed some common scams involving the pandemic. Most of these scams pertained to bogus relief checks, fictitious online ads for vaccines, and sellers that had stockpiles of "hot-ticket" items, such as disinfectant wipes, that they were trying to unload. While these scams are still present more than a year later, the true uptick, actually, relates to fake emails about proof of vaccination, being laid off, and health organizations that request personal information.

More specifically, waves of companies have reported seeing phony Office 365 emails from "Human Resources," which ask employees to submit information regarding their vaccination status. Should one decide to click on the malicious link within this email, the employee would be redirected to a page that looks strikingly like a Microsoft login. If the recipient elected to type an email address and password into this fake page, these credentials would be stolen in the background.

Next, employees of many organizations have also confirmed receiving phishing emails that discuss their termination, often citing pandemic hardships. It is expected that one would be in an emotional state after getting an email of this nature, so, without thinking, the recipient might open a malware-laced attachment of an alleged severance package.

The last type of these newer scams is an email purporting to be from the "CDC," "WHO," or a local health department. Within these particular emails, the "CDC," for example, will ask you to verify your identity. The goal behind this phishing email is to get the recipient to provide personal information, such as a Social Security number, or a copy of a vaccination card, etc., with the sender hoping to sell this critical PII on the Dark Web.

Even more alarming than the above scams is how rampant they are. For example, Google alone, on a daily basis, examines 18 million COVID-19 themed malware/phishing emails and 240 million COVID spam messages for its users. Since the beginning of the pandemic, consumers have lost more than $552M to COVID-19 phishing emails. Unfortunately, forecasters anticipate this trend will continue. Therefore, as with all phishing emails, please review the red flags below, which can help in determining whether an email is legitimate:

- Check for grammatical mistakes within the email and odd sentence structure.
- Look for generic introductions:
  - "Hello, kindly review," "Dear customer," "Hi, see attached," etc.
  - The same can be said for formal salutations, such as "Sir," and "Madam."
- Examine unusual senses of urgency:
  - "Click on the below link ASAP to begin the process."
- Hover over ALL links. If you receive an email from the CDC with a link within the email, make sure it goes out to the intended site.
  - For example, a URL inside an email can read, "*CDC Vaccination Information*." However, when the link gets hovered over, it goes to a random website that apparently has no affiliation with the CDC.
- Be wary of attachments that are URLs.
  - PDF attachments that are hyperlinked are common offenders.
- Ask yourself, "Was I expecting something from this sender?"
  - In many cases, phishing emails are completely unexpected.
    - If this is the case, do not be afraid to call the sender using a *known* number and not one found within their signature line, as these can be altered.

Statistics and information were derived from ZDnet.com, trendmicro.com, aarp.org, and theverge.com.

Please contact CATICITSecurity@catic.com if you have any questions.