COVID-19 Vaccine Themed Phishing Emails

Executive Summary

There is an increased risk of COVID-19 vaccine-themed phishing emails with the release of the vaccines to the public. It is anticipated that in addition to emails, criminals will use malicious websites, phone calls, text messages, social media, and door-to-door in-person interactions to contact their intended victims. Suspect emails may contain alternate treatments, request payment or personally identifiable information, or promise early access to the vaccine. Mitigations to phishing emails are provided below.

Analysis

Criminal actors will continue to use COVID-19 as a theme for phishing emails. With the release of COVID-19 vaccines it is anticipated that criminals will focus their COVID-19 themed emails on vaccine-related lures. COVID-19 vaccine-themed phishing emails will likely continue to be a threat throughout the duration of the global push towards vaccination.

Alert

As of early December 2020, government and private organizations warned about the increased risk of COVID-19-related phishing attempts as vaccines become available. In addition to phishing, the Better Business Bureau anticipates scammers reaching out via other means such as phone calls, text messages, social media, and door-to-door in-person interactions to contact their intended victims. The Federal Bureau of Investigation (FBI) specifically advised for increased caution during the "initial supply-and-demand problem" that will occur when the limited supply of COVID-19 vaccines become publicly available. During this time the FBI expects bad actors to use telemarketing, malicious websites or emails to contact their intended victims.

Another risk that could make the COVID-19 phishing emails seem more realistic is the possibility of criminal organizations developing black market vaccines for sale. In October 2020, Mexican criminal groups sold counterfeit flu vaccines in bottles that appeared identical to the real vaccines. However, the batch numbers and expiration dates differed from the legitimate product. Additionally, some vendors on the dark web are already selling purported COVID-19 vaccines.

According to the Federal Trade Commission's Division of Consumer and Business Education, emails containing alternate treatments, requesting payment or personally identifiable information, or promising early access to the vaccine would be suspect:

- You likely will not need to pay anything out of pocket to get the vaccine during this public health emergency.
- You can't pay to put your name on a list to get the vaccine.
- You can't pay to get early access to the vaccine.
- No one from a vaccine distribution site or health care payer, like a private insurance company, will call you asking for your Social Security number, credit card, or bank account information to sign you up to get the vaccine.

The Rhode Island Department of Health issued a warning on their Facebook page about a COVID-19 vaccine-themed email that purported to be from a department physician "with a COVID-19 vaccine pre-registration link and email."

Any instances of scams, fraud, and bad business practices can be reported online at reportfraud.ftc.gov.

Patches, Mitigations & Workarounds:

Recommended actions to protect against phishing attacks are:

- User awareness and training to help identify and avoid phishing scams
- Operationalization of Indicators of Compromise (IOCs)
- Automatic banners for any e-mails that originate outside the organization
- Use of blacklisting of malicious sites and whitelisting for known, trusted sites
- Integration of anti-spoofing technologies such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC)
- Update operating systems and applications with the latest security updates, including third-party software
- Implement and update endpoint security systems

References

Tafoya, Bernie. "BBB: Beware of COVID vaccine scams." WBBM News Radio. December 14, 2020. https://www.radio.com/wbbm780/news/local/bbb-beware-of-covid-vaccine-scams

Barr, Luke. "FBI warns of COVID-19 vaccine scams." ABC News. December 9, 2020. https://abcnews.go.com/US/fbi-warns-covid-19-vaccine-scams/story?id=74631650

European Union Agency for Law Enforcement Cooperation (EUROPOL). “Vaccine-related crime during the COVID-19 pandemic.” EUROPOL. December 4, 2020. https://www.europol.europa.eu/publications-documents/early-warning-notification-vaccine-related-crime-during-covid-19-pandemic

Tressler, Colleen. "COVID-19 vaccines are in the pipeline. Scammers won’t be far behind." Division of Consumer and Business Education, Federal Trade Commission. December 8, 2020. https://www.consumer.ftc.gov/blog/2020/12/covid-19-vaccines-are-pipeline-scammers-wont-be-far-behind

Rhode Island Department of Health (RIDOH). “RIDOH has become aware of an identity theft scam…” RIDOH. December 8, 2020. https://www.facebook.com/HealthRI/posts/4897359040304716?__tn__=-R

Health Sector Cybersecurity Coordination Center (HC3). "Coronavirus Themed E-mail Phishing." HC3, Department of Health and Human Services. February 3, 2020. https://www.hhs.gov/sites/default/files/coronavirus-themed-email-phishing.pdf