From the desk of
Michael Aliperti
MS-ISAC Chair

Top 4 COVID-19 Scams to Watch Out For

The ability to leverage current events is a dream scenario for modern-day cybercriminals. These criminals use events, such as the COVID-19 pandemic, to fuel their malicious intent.

With the global pandemic comes the desire to stay updated with the most current information. However, it can be difficult for internet users to navigate this information and separate fact from fiction. It is also difficult to ensure that links and resources are reliable. The reality is that malicious activity comes through just about every communication channel: email, social media, text and phone messages, and of course, misleading and malicious websites.

Here are some common examples of what you need to be on the lookout for in the months to come:

1. Malicious Websites

Throughout the COVID-19 pandemic, cyber threat actors have consistently capitalized on global interest surrounding the latest information on the virus. These threat actors take advantage of internet users by registering website domains related to COVID-19. Fake websites and applications typically claim to share news, testing results, or other resources, however, they ONLY want your credentials, bank account information, or to infect your devices with malware.

With many organizations and employees continuing to work from home, users may let their guard down and be more susceptible to emails from unverified senders. NEVER give out your personal information, including banking information, Social Security Number, or other personally identifiable information (PII) over the phone or email.

2. Phishing Emails

Expect phishing emails to be on the rise Cyber threat actors will utilize COVID-19 phishing emails in an attempt to convince the recipient to either reveal sensitive information (i.e. bank account information), or simply try to convince the recipient to open a malicious link or attachment, allowing them to potentially access your system.

COVID-19 vaccine-themed phishing emails may include subject lines such as the following:

- Vaccine registration
- Information about your vaccine coverage
- Locations you can receive the vaccine
- Ways you can reserve a vaccine
- Vaccine requirements

While some phishing emails might be easy for you to detect, never get complacent when reviewing your emails. Expect to receive well-composed phishing attempts that are impersonating well-known and trusted entities, such as government agencies, healthcare providers, or pharmaceutical

companies. NEVER open any link or attachment from a source that you cannot clearly identify as being legitimate!

For instance, email phishing campaigns in the past have targeted state-level agencies impersonating the Centers for Disease Control and Prevention (CDC). These emails have requested recipients to click on links in order to view a secured message pertaining to COVID-19 vaccine information. Links such as these could easily direct the user to a webpage that attempts to collect PII, including name, address, date of birth, driver's license number, phone number, and email address.

Here are some notable indications an email, text, or phone call may be a phishing attempt:

- Inspiring a sense of urgency to click a link or provide information
- Is overly formal or written in an overly complicated manner
- Requests sensitive information or that you review a link or attachment

Asks users to follow a non-standard process, or a process you might find odd!

3. Fraudulent Charities

For as long as the pandemic is around there will always be consistent attempts by threat actors to create fraudulent charities seeking donations for illegitimate or non-existent organizations. Fake charity and donation websites will try to take advantage of one's good will, especially during such hard times. Always do your research before donating and providing any information.

4. Unemployment Scams

As tax season is quickly approaching, be wary of identity theft scams involving fraudulent claims, especially surrounding unemployment benefits. This scam has especially skyrocketed during the COVID-19 pandemic as unemployment claims in general have been on the rise. The most typical scams to be on the lookout for (but are not limited to) include telling recipients that they've won contests, a cash prize, or are eligible for an award for applying for unemployment.

Recommendations

Phishing remains a prominent attack vector for almost all cyber threat actors. Your cybersecurity best practices will always be your first line of defense against phishing. Here are some recommendations you can take to shield yourself from these threats:

- Establish a properly-configured firewall
- Ensure your internet-connected devices are not connected to any public internet
- Report any suspicious emails to your organization's IT department
- Enable strong authentication tools, such as Multi-Factor Authentication (MFA).
  - To learn how to activate MFA on your accounts, head to Stop.Think.Connect.: https://stopthinkconnect.org/campaigns/lock-down-your-login
    - Lock Down Your Login provides instructions on how to apply this tool to many common websites and software products you might use
  - Continuously update your passwords and update any default unsecure settings Ensure backup protocols are in place with your devices
  - NEVER give out your personal information, including banking information, Social Security Number, or PII over the phone or email
  - Always verify a charity's authenticity before making donations. For

assistance with verification, utilize the Federal Trade Commission's (FTC) page on Charity Scams. This information can be found here: https://www.consumer.ftc.gov/articles/0074-giving-charity

If you suspect you've been impacted by a scam or attempted fraud involving COVID-19, you can file a report with the Cybercrime Support Network. More information can be found here: https://cybercrimesupport.org/covid-19-scam-alerts/

Additional Resources

- CDC | COVID-19-Related Phone Scams and Phishing Attacks (https://www.cdc.gov/media/phishing.html)
- CISA | Insights (https://www.cisa.gov/insights)
- CISA | Information & Updates on COVID-19 (https://www.cisa.gov/coronavirus)
- DHS | Operation Stolen Promise (https://www.ice.gov/topics/operation-stolen-promise)
- FDA | Beware of Fraudulent Coronavirus Tests, Vaccines and Treatments (https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments)
- U.S. DOJ | Coronavirus (https://www.justice.gov/coronavirus)