COVID-19 & CYBERSECURITY

mxo tech
Beyond IT. People.

Fear for Sale: Hackers Using Coronavirus Concerns to Spread Malware

What if a physical virus wasn't the only virus you needed to fear? Welcome to the constantly evolving world of cybercrime, where the current trend is hackers using coronavirus concerns to spread malware.

From click-bait "epidemic maps" to phony websites, here are the things you need to know to keep your network safe.

Fake CDC or WHO Updates

There is nothing more trusted in times of trouble than government organizations such as the Center for Disease Control, the National Institute of Health, or the World Health Organization.

One growing trend among cybercriminals is an email, allegedly from the CDC, urging readers to click a Microsoft Office document to see important details on how to stop the spread of contagion, such as flu or coronavirus. The CDC has issued a warning along with an example of how this email would appear to users.

Other phishing attacks can involve "tips" for COVID-19 protection, or a supply list for self-quarantine.

Stay Safe: No official governmental health organization will ever send you unsolicited emails regarding any disease or epidemic, nor will they ever force you to log in to receive updates. To stay on top of coronavirus announcements, type the organization's name into your browser and access it directly.

Hackers Using Coronavirus Concerns to Promise Cures

Hackers are targeting email users with promises of a cure for coronavirus. Some of these offer tips, while others may contain links to purchase these "cures." Others hint at a vaccine available "in your area," or testing information.

Clicking these sites can infect your network. Additionally, your employees may be tempted to purchase these cures, sending money directly to the scammers themselves.

Stay Safe: To date, there is no vaccine or cure for coronavirus. Remind your employees not to send financial information to any site promising a cure or vaccine.

False "Maps"

Hackers using coronavirus fears have developed realistic looking maps to track the spread of the infection. Once clicked, these maps will spread malware throughout your network.

Remember that no trustworthy organization is sending you COVID-19 information via email.

Stay Safe: To be safe, search maps in your browser and only go to sites that are well-known and respected, such as Johns Hopkins University or the New York Times.

Falsified Employer Health Policies

Hackers using coronavirus opportunities will draft a blanket email to your employees, requesting they click a link to view your company's "COVID-19 policies." While most companies have drafted policies, they will be sent from trusted sources and CEO's, not anonymous or generic senders such as "Human Resources."

Stay Safe: Give your employees instructions to view your COVID-19 in a shared document platform such as Teams, or share it via printed documents.

Discount Supplies

You may start receiving ads from unfamiliar sites promising discounted coronavirus supplies and protections, such as gloves, masks and hand sanitizer. The emails may contain links to "discount codes" and shopping pages.

Scammers Get Your Financial Data

When you click the links for discounted supplies from unfamiliar sites, you can potentially infect your network with malware. This malware can cripple your network or collect information on your employees and customers.

Pay for Nothing

Clicking an untrusted "online store" allows cybercriminals to directly access your financial information by having you "order online." In return, you will either receive cheap items or, in most cases, nothing at all. By the time you realize you have been duped, these sites are already taken down and untraceable.

Stay Safe: Only shop the online stores you trust, and always access them directly through your browser.

Asking for Donations

Another email tactic of hackers using coronavirus scams will involve asking readers to donate money to organizations that are allegedly "looking for a cure" or "helping those affected by coronavirus." Users are urged to click a link taking them to the site or to provide financial information for their donation.

Stay Safe: At present, the WHO has only one resource for COVID-19 donations, the COVID-19 Solidarity Response Fund, and the CDC encourages donations to the CDC Foundation's Emergency Response Fund. Take the time to investigate charitable organizations and only give to those you trust.

Tax Refund Scams

The timing of COVID-19 coincides with tax season, and hackers know it. Some emails are promising tax-burden relief for those living in areas heavily affected

by the coronavirus or for families who are missing work opportunities because their employers have temporarily closed their doors.

Stay Safe: Remember, the IRS will never send unsolicited email. Stay informed from news outlets and never click on anything that sounds too good to be true.

Why Would People Fall for COVID-19 Phishing Scams?

When faced with a crisis such as the COVID-19, fear can make even the most cyber-savvy individuals forget common cybersecurity practices. The urge to stay safe and informed is at the front of peoples' minds, often pushing aside security considerations.

Hackers using coronavirus fears are taking the game to new levels by promising cures, hard-to-find preventative equipment and supplies, and updated information to play on the uncertainty, misinformation, and fear associated with COVID-19.

Hackers are increasingly becoming more sophisticated in their approach, making these emails and "updates" appear incredibly realistic. Coronavirus emails appear to come from official sources to increase a reader's trust and decrease suspicion.

It can go one step further than just the emails alone; spoofing websites can accompany these emails with official looking pages as well.

Cybersecurity Safety Reminders

Hackers using coronavirus concerns as phishing attempts is on the rise and will probably continue to increase over the coming weeks.

This is the time to remind your employees about cybercrime and phishing, whether they are working from the office or remotely.

Never

- Open any email from an unrecognized source
- Open an email that is allegedly from a governmental organization, such as WHO, the IRS, or the CDC
- Click on any link from a source you don't recognize
- Open an email with generic headings or misspelled subject lines

Always

- Access websites directly via a browser
- Report suspicious emails to your IT department
- Be wary of websites or emails with grammatical errors, misspelling, or foreign sounding phraseology
- Question the sender of organizational policies or procedures via email to be certain it came from them
- Log in to trusted websites for information and updates on COVID-19

Feel free to use this MXOtech article for your workforce to remind them to stay safe. If you have any questions or concerns, please don't hesitate to contact our team directly at 312.554.5699 or at sales@mxotech.com.