Coronavirus COVID-19 fraud: companies face new phishing attacks

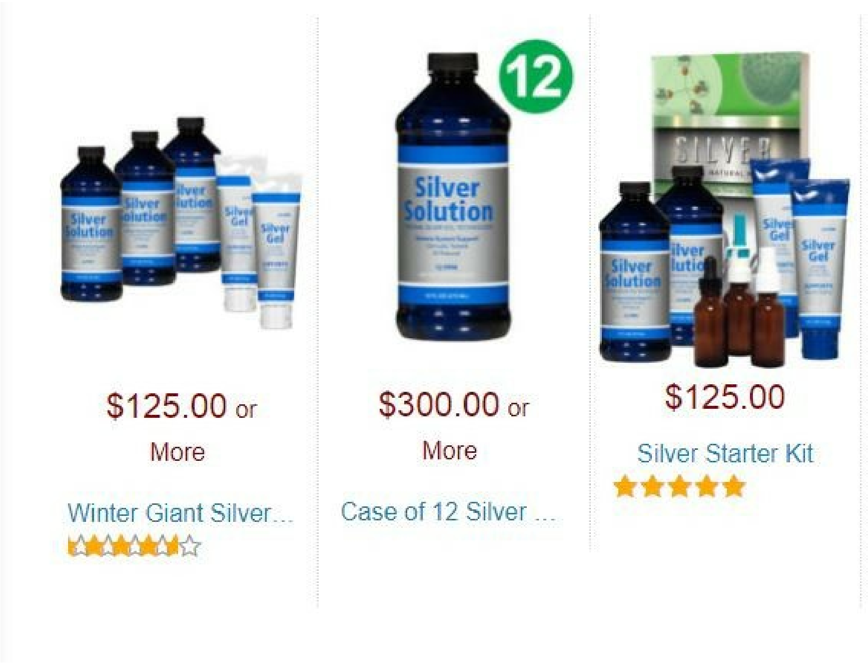
blog.barracuda.com/2020/03/11/coronavirus-covid-19-fraud-companies-face-new-phishing-attacks/

Olesia Klevchuk

March 11, 2020March 24, 2020

As Coronavirus COVID-19 makes its way across the world, individuals are doing their best to stay up-to-date on the latest outbreak locations and confirmed cases. Hackers have created new attacks based on the intense public interest in this virus.

One of the most common of these attacks is an email impersonation attack. In this attack, the criminal impersonates organizations like the UN World Health Organization (WHO) and the US Centers for Disease Control and Prevention (CDC) to trick users into opening a malicious email. Multiple government organizations have issued warnings against these attacks.



$125.00 or More

Winter Giant Silver...

$300.00 or More

Case of 12 Silver ...

$125.00

Silver Starter Kit

Fake ‘Silver Solution' Coronavirus Cure Sued by Missouri AG

Email scams always follow the headlines

It’s not unusual for hackers to monetize on tragedies like hurricanes and other disasters. Most of these scams are designed to do some variation of the following:

- Infect the user device and spread malware
- Steal login credentials by way of a phishing site or other phishing mechanism
- Collect donations for fake charities through malicious websites

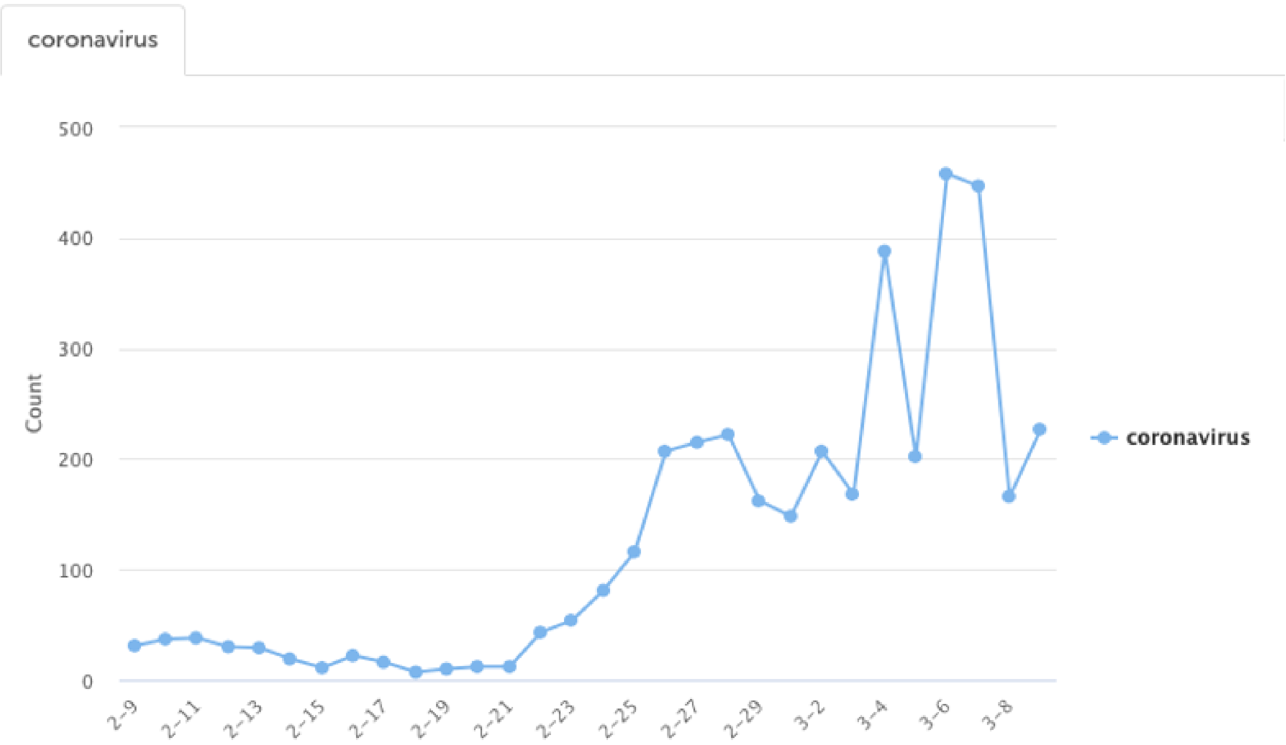
The current pandemic has given scammers all those opportunities and more:

- Selling counterfeit versions of medical supplies that are in short supply
- Tricking users into buying fake cures
- Offering investment opportunities in companies claiming to have the cure

Email scammers will continue to find new ways to take advantage of the Coronavirus COVID-19 pandemic. If you have the proper email protection in place and you know what to watch out for, you can protect yourself from these email attacks.

Spreading the infection

There has been a real surge in the registration of new domains that use the word ‘coronavirus.’ Some of these will be put to a good use, but many will be used by hackers for malicious purposes. These malicious websites might appear to offer news or advice on coronavirus outbreak but are being used for phishing or to spread malware. Email impersonation scams often include links to this type of site.

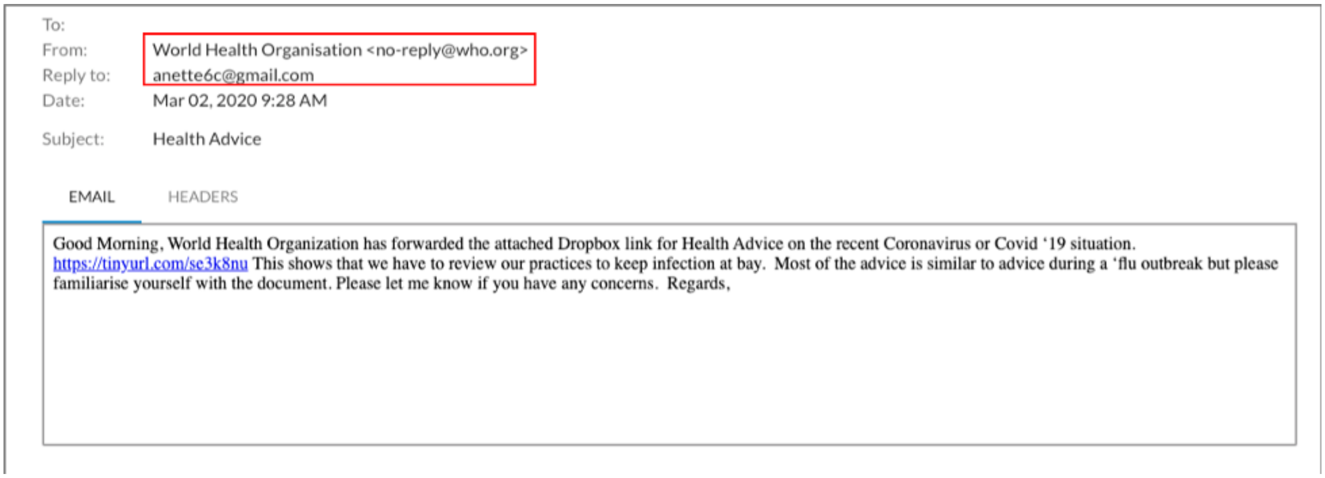


Domain registrations with the word “Coronavirus” Source: Verisign

Email impersonation attacks

Over the past few weeks, we have seen a number of attacks impersonating the World Health Organization. These phishing emails appear to come from WHO with information on Coronavirus COVID-19. They often use domain spoofing tactics to trick users into thinking these messages are legitimate.

These email impersonation attacks will include a link in the body of the email. Users who click on that link are taken to a newly registered phishing website.

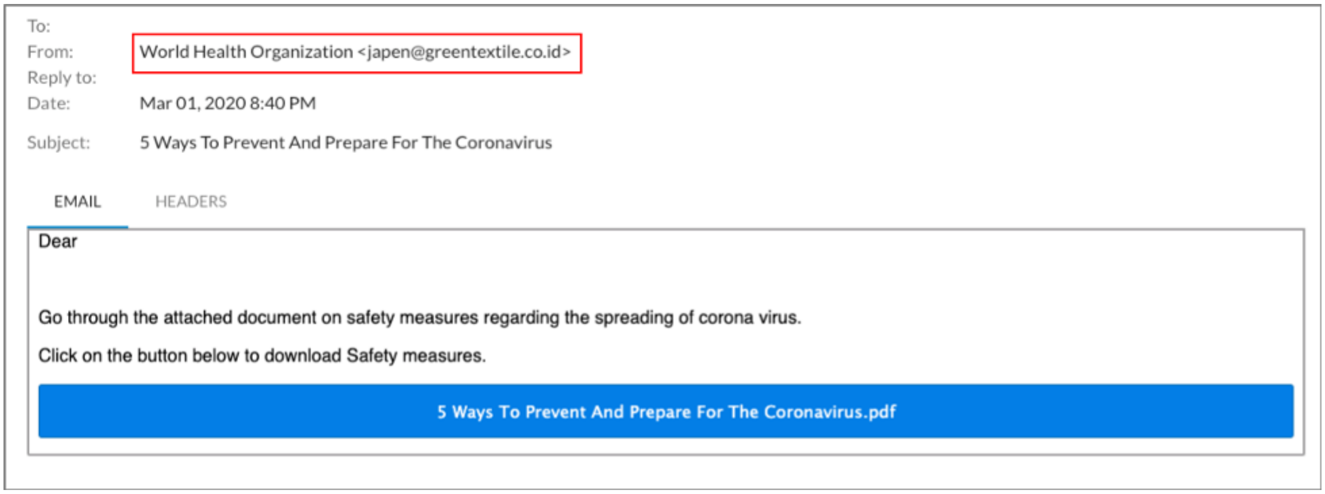


To:
From: World Health Organisation <no-reply@who.org>
Reply to: anette6c@gmail.com
Date: Mar 02, 2020 9:28 AM

Subject: Health Advice

EMAIL HEADERS

Good Morning, World Health Organization has forwarded the attached Dropbox link for Health Advice on the recent Coronavirus or Covid ‘19 situation. https://tinyurl.com/se3k8nu This shows that we have to review our practices to keep infection at bay. Most of the advice is similar to advice during a ‘flu outbreak but please familiarise yourself with the document. Please let me know if you have any concerns. Regards,



To:
From: World Health Organization <japen@greentextile.co.id>
Reply to:
Date: Mar 01, 2020 8:40 PM
Subject: 5 Ways To Prevent And Prepare For The Coronavirus

Dear

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download Safety measures.

Remote work and increased risk

As a preventative measure against the spread of Coronavirus COVID-19, many organizations are asking employees to work remotely from home until further notice. These remote workers may rely on email for communication with other employees as well as updates on workplace location and other issues related to the outbreak. This puts users in a state of expectation for email messages from HR or upper management on the subject of the virus. This expectation creates an increased risk for the company because the user is more likely to accidentally open a malicious email if they are expecting a similar legitimate message.

These factors, combined with the diminished ability to confirm the legitimacy of an email due to remote working is a perfect environment for email scams.

Protecting your organization and employees

There are several ways to protect your company and employees from email scams, and they are based on employee education and security technology:

- Don’t click on links in email from sources you do not know; they may lead to malicious websites
- Be wary of emails claiming to be from the CDC or WHO. Go directly to their websites for the latest information.
- Pay special attention to email messages from internal departments or executives who sent regular updates on the outbreak. Domain and display name spoofing are some of the most common techniques used.
- Never give personal information or login details in response to an email request. This is how a phishing attack leads to business email compromise.
- All malicious emails and attacks should be immediately reported to IT departments for investigation and remediation.

- Ensure that your organization has reliable virus, malware, and anti-phishing protection.
- Make sure employees receive up-to-date training on the latest phishing and social-engineering attacks.

Criminals are always looking for new ways to exploit the latest tragedies. Keep up on the latest scams by following alerts from CISA and similar sites.

Related:

- Secret Service Issues COVID-19 (Coronavirus) Phishing Alert
- Defending Against COVID-19 Cyber Scams
- Retailers beware: Coronavirus scams are popping up everywhere