Please share with your employees!

Currently, attackers are using coronavirus themes for nearly all types of attacks, including (but not limited to) business email compromise, credential phishing, malware, and spam email campaigns.

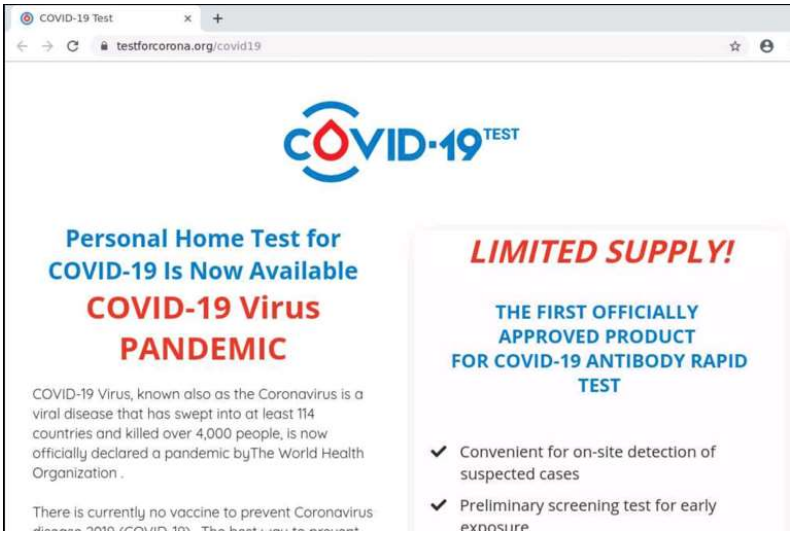
Attackers are actively abusing the names and logos of many companies and organizations within these campaigns in an attempt to manipulate recipients. Of particular note is the spoofing and brand abuse of national and international health organizations around the world, including the World Health Organization (WHO), the United States Centers for Disease Control (CDC), and Canadian and Australian national health organizations.

These bad actors are preying on users' emotions of fear and uncertainty. The best way for all of this to be avoided is to be sure to tell your employees DO NOT CLICK!

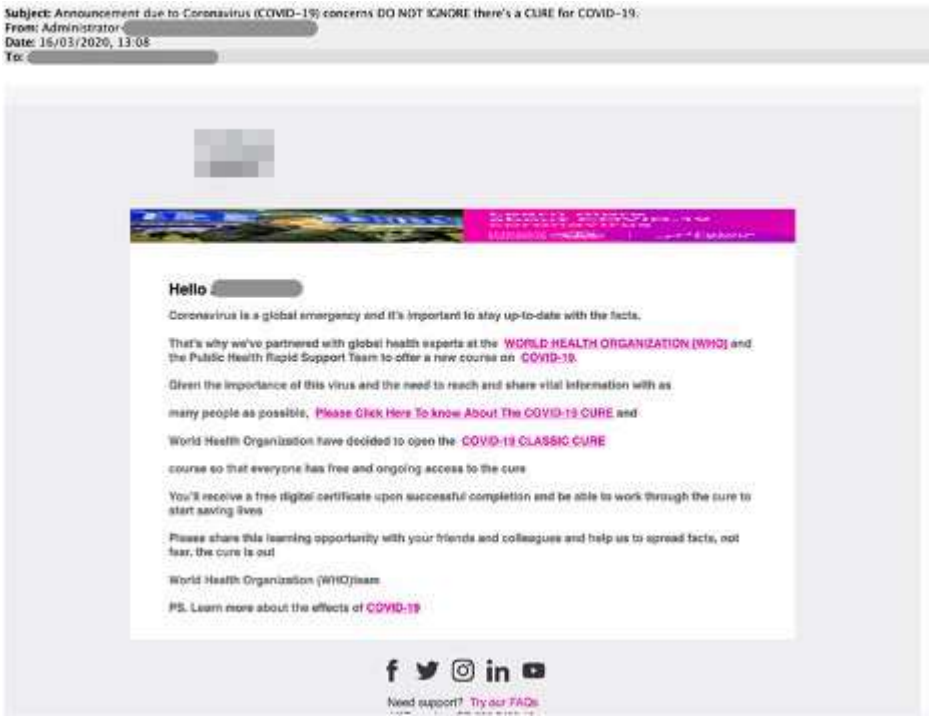
If your employees receive an email from any source, including if it loos like it's coming from an internal person of authority and it seems out of sort, they should never click on any links or open any attachments from that email and reach out to the sender to verify if they actually sent it.

Here is a sample of some of the scams that are active around the world:

- **Take the test:** Several scams offer DIY "at home" coronavirus tests leading to fake testing sites that can capture credit card information. The fake site in the accompanying image was spotted by Mimecast Threat Intelligence. Only one company has announced a legitimate at home coronavirus test, which is set to hit next week.



- **WHO's calling:** Email scammers pretend to be the World Health Organization offering information on how to avoid infection. When you click through, it asks for personal information.[i] There's only one official WHO site: WHO:int. WHO also has a page that provides information about how to avoid scammers pretending to be them.



- **Get educated about the (phony) cure**: The phishing scammers in the accompanying screen capture pretend to be a well-known online learning company offering a course to teach you all about the cure to COVID-19, but they harvest your credentials instead (if you let them). It sounds more legitimate by claiming partnership with the WHO.

- **CDC Imposters**: The Centers for Disease Control and Prevention is unlikely to email individuals with offers of any kind. But the real CDC coronavirus site is a valuable source of critically important information.

- **Free Phones:** This one's an SMS, not email, scam. Forbes reports that a congresswoman received a supposed offer of free iPhone 11s from Apple "to help you spend time at home."[ii] Apple is not giving away free phones.

If your employees receive an email they're not sure of, the best action is to NOT CLICK on any attachments or links and delete the email. If they think the email may be valid but they're not 100% sure, they should not click on any links, but keep the email and then reach out to us at help@nens.com. Please do not forward the email to us. We will connect to their machine remotely and review the email with them to determine its authenticity.

As always, stay safe and don't hesitate to contact us if you have any questions.

Sincerely,

Jason Bricault
Director of Remote Services & Network Operations