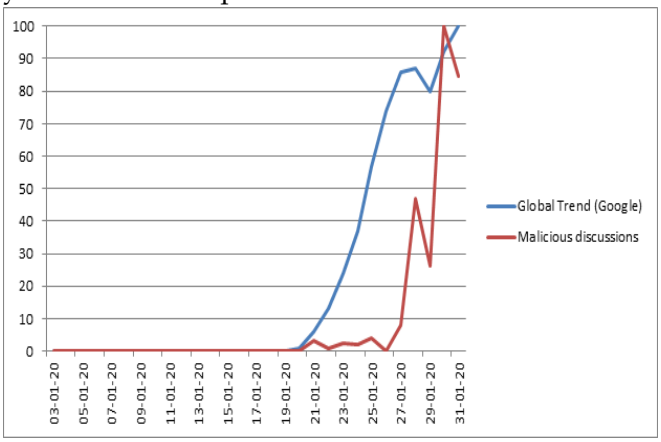
Scammers And Cybercriminals Are Always On The Hunt for new ways to deceive and harm people. The days of Nigerian Princes who need help moving money may be fading, but newer scams are cropping up each month.

Popular phishing and malware scams tend to follow global trends and current events. This isn't a coincidence. A timely cover story is far more likely to attract victims than random scenarios. **Tap or click to see how malware and scams spread after the holidays.**

And right now, no story is timelier than the coronavirus epidemic. People around the world are looking for ways to protect themselves from the virus, and scammers are claiming to have the answer. If you fall for the scam, you might even end up with a virus yourself — a computer virus!



Digital snake oil: The newest plot for online scammers and cybercriminals

Bogus cures, vaccines, face masks and home tests for the novel coronavirus are being spotted online with increasing regularity. It's all part of the latest wave of cyberattacks and scams featuring the real-world epidemic — a phenomenon that started in Japan and has since spread worldwide.

You may also like: See the previous wave of coronavirus email scams and phishing attempts

According to security researchers at **Check Point Software Technologies**, cybercriminals have been using the coronavirus news trends to spread malicious software and scams.

In a graph posted to Check Point's blog, a sharp spike in malicious coronavirus discussions closely trends with Google searches and news mentions.

Check Point Software Technologies LTD

Since the jump, Japanese netizens have been bombarded with spam emails masquerading as public bulletins about local infections in the victims' areas. These messages contain a type of Trojan virus called Emoted, which is capable of reproducing itself once it infects a system.

But Japan isn't the only country dealing with malicious coronavirus activity. In the past two months, more than 1,000 coronavirus-themed website domains were registered. Many of these appear to be phishing domains, while others are scam websites that offer bogus goods and services.

For example, this Russian domain claims to offer the fastest coronavirus detection test for the low, low price of just 19,000 rubles, which is approximately $300 U.S. Dollars. An absolute *steal*. This same website also spreads sensationalized news that misinforms victims.

Check Point Software Technologies LTD

The website also appears incomplete, with English-language placeholder text all over the place. Are Russian hackers even trying anymore?

Check Point Software Technologies LTD

Despite the poor effort from Russian cybercriminals, that doesn't mean attempts from elsewhere will be as obvious or clunky. As more cases of the actual virus emerge, expect to see a greater uptick in coronavirus-themed malware, phishing emails and fake news.

RELATED: Tap or click here to see if you can tell the real coronavirus news stories from the fake ones.

How can I protect myself from coronavirus scams and malware?

As with any kind of cybercrime, vigilance and skepticism are your best friends. Never open emails you don't recognize and especially avoid downloading any kind of attachments unless you're 100% familiar with them. Doing so opens your system up to unnecessary risks.

Additionally, avoid any "special offers," like exclusive coronavirus cures or dirt-cheap deals on protective gear and technology. Check Point also advises checking the URLs and domains of websites for obvious spelling errors, which can be red flags.

At this point, scams are becoming harder to detect. But if you stay informed, your knowledge will be the most powerful defense you could ask for.

(Source: KinKomando.com)