

Hackers are using coronavirus fears to send you a computer virus: How to stop them

February 4 2020, by Dalvin Brown



Credit: CC0 Public Domain

As the coronavirus continues to spread across the globe sickening thousands of people in its wake, a malicious strain of software is seeking to take advantage of people's fears.

Researchers with IBM X-Force and Kaspersky have discovered that hackers are sending spam emails to people in the hopes of infecting smartphones and computers with malicious software.

The malware is disguised as legitimate information about coronavirus.

The emails sent to people in Japan claim that the respiratory illness has infiltrated the country, and urge the receiver to open an [email](#) attachment to learn more information. If the receiver opens the file, malicious software harvests personal data and can inject other inflammatory software.

That means hackers can gain access to your personal files and copy them.

"We have observed several instances of such exploitations in the past and now detected a recent wave, motivated by the outbreak of the coronavirus in China," cybersecurity researchers at IBM said in the report, adding that this approach may be more successful due to fear of infection surrounding coronavirus.

Hackers often use [current events](#) and compelling verbiage to get people to open emails, download attachments or tap links. Since coronavirus is hot a topic, it's no surprise that bad actors would use the widespread illness to prey on people's fears, experts say.

"Hackers will use whatever is timely to get victims to do the action required," said Marty Puranik, a cybersecurity expert and CEO of Atlantic.Net, which instructs people on how to avoid getting their information compromised.

Hackers also track the open and install rates of their various malware campaigns, so they can scale and reproduce the scams that perform the

best for them, Puranik added.

IBM's report focuses primarily on Japan, though there could be an uptick in malicious coronavirus-related scam emails in the U.S. too.

"We expect to see more malicious email traffic based on the coronavirus in the future, as the infection spreads," IBM said in the report. "This will probably include other languages too."

Hackers get savvier over time, however, there are things you can do to thwart coronavirus-related attacks and other hacking attempts.

Always exercise caution. Don't open sketchy links sent to you via text or email. Don't answer suspicious phone calls, and don't download attachments that you didn't ask for.

"If you want to learn more about coronavirus, you can search Google and find a safe site that can advise you on the matter," Puranik said.

Be sure to only install official updates. In 2019, millions of Android phones were reportedly infected with malware through a fake Samsung app.

Use secure passwords. Ring security cameras were hacked, and short, easy-to-guess passwords may have been the reason why. Two-factor authentication is always a good idea.

Run anti-virus software on your smartphone. These apps protect your device from viruses and other malware, and premium services lock down your privacy settings and scan apps and files for security threats.

(c)2020 U.S. Today

Distributed by Tribune Content Agency, LLC.

Citation: Hackers are using coronavirus fears to send you a computer virus: How to stop them (2020, February 4) retrieved 3 May 2024 from <https://techxplore.com/news/2020-02-hackers-coronavirus-virus.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.