Unfortunately bad actors are leveraging the current Coronavirus epidemic for malicious intent. It has escalated so quickly that the United States Secret Service issued a press release.

As you might imagine, the phishing attacks exploit our concerns regarding COVID-19.

One widespread campaign includes a poisoned PDF document labelled “CoronaVirusSafetyMeasures_pdf” which, if opened, can give full administrative control of your computer to the attacker.

Another uses a three-page coronavirus-themed Microsoft Office document purported to be from the Center for Disease Control to drop a backdoor onto a victim’s computer. The fake message includes calls to urgency; “the coronavirus has officially become airborne” and there “have been confirmed cases of the disease in your location.”

Accordingly, it is critical that you follow good email practices. If you have the slightest doubt about an email, DO NOT OPEN IT. Instead, please contact the help desk for instructions.

Another area of concern is malicious COVID-19 websites.
Check Point Threat Intelligence has identified over 300 websites that are malicious/suspicious.

**Corona virus maps are being used to compromise systems.**

Accordingly, we recommend that you only visit well known sites (e.g., CDC.gov, nytimes.com, etc.) for your corona virus news.

**Working from home also potentially increases your exposure to “vishing” attacks.**

Beware calls from Microsoft or your Internet Service Provider that indicate that there is a problem with your connection (e.g., poor quality, your machine is sending malicious data, etc.). Their intent is to gather information about you and your systems with the ultimate goal of getting you to allow them to connect to your machine remotely to “troubleshoot” the issue.

Accordingly, do not give out information to any party calling without positively identifying them. The best approach is to call them back at a number you find listed on that companies website.

Please report any phishing or vishing attacks immediately to the help desk. Stay healthy & safe, both physically & digitally.

COPYRIGHT © 2020, STARK & STARK

**Source URL:** [https://www.natlawreview.com/article/possible-security-risks-working-home](https://www.natlawreview.com/article/possible-security-risks-working-home)