1 ADP Boulevard
Roseland, N.J. 07068

Date: March 13, 2020
From: ADP Global Security Organization
Subject: Coronavirus Scam Alert: Watch out for these risky COVID-19 Websites and Emails

---

Cybercriminals are using concerns about the coronavirus to launch phishing attacks.

What Happened?

While COVID-19, or the novel coronavirus, is capturing attention around the world, cybercriminals are capitalizing on the public's desire to learn more about the outbreak. There are reports of phishing scams that attempt to steal personal information or to infect your devices with malware, and ads that peddle false information or scam products.

In one example, a phishing email that used the logo of the CDC Health Alert Network claimed to provide a list of local active infections. Recipients were instructed to click on a link in the email to access the list. Next, recipients were asked to enter their email login credentials, which were then stolen.

What Should You Do:

1. If you are looking for information on the coronavirus, visit known reputable websites like U.S. Center for Disease Control or the World Health Organization.
2. Be on the lookout for phishing emails which may appear to come from a trusted source. Remember, you can look at the sender's details – specifically the part of the email address after the '@' symbol – in the 'From' line to see if it looks legitimate.
3. Be wary of emails or phone calls offering unexpected or unprompted information. Also be aware of emails from unfamiliar sources that contain links or attachments. Do not click on these links, as they could be embedded with malware.
4. Although social media companies like Facebook are cracking down on ads spreading coronavirus conspiracies and fake cures, some ads may make it past their review process. Remember, it's best to seek information on the disease from official sources like those mentioned above.

ADP will not request sensitive personal information such as Social Security Numbers, login credentials, or bank or credit card information via unsolicited phone, email, or internet-based communications. If this information is ever requested in a communication that you did not initiate, it is an indicator of a scam.

Clients are encouraged to visit our website at www.adp.com/trust to learn more about how ADP protects data, and how clients can help protect themselves. Protecting our clients and their data from malicious activity is a top priority for ADP.

Sign up to have new alert notifications delivered to you by email – visit the alerts section of www.adp.com/Trust for more information.

Resources: from Lifelock