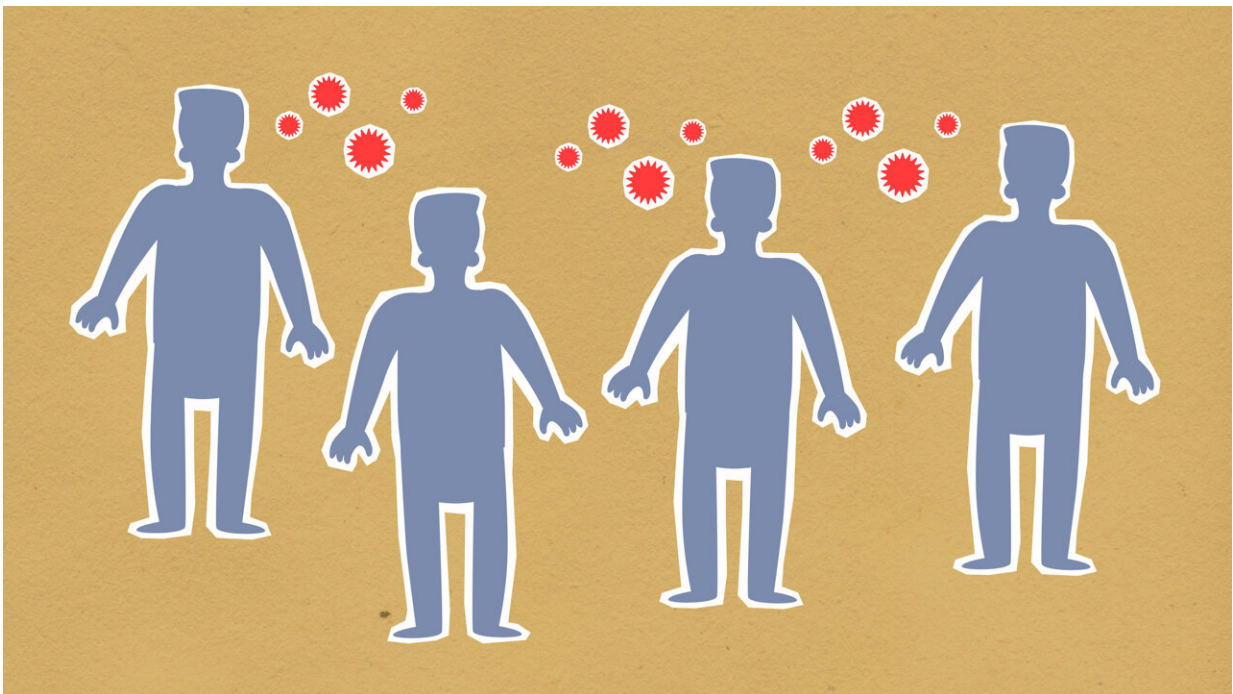# Coronavirus pandemic has unleashed a wave of cyber attacks: How to protect yourself

April 1 2020, by Chaminda Hewage

Credit: Monstera Production from Pexels

While most of the world is trying to deal with the COVID-19 pandemic, it seems hackers are not on lockdown. Cyber criminals are trying to leverage the emergency by sending out "phishing" attacks that lure internet users to click on malicious links or files. This can allow the hackers to steal sensitive data or even take control of a user's device and use it to direct further attacks.

The last thing you want at a time like this is to become a victim of a cyber attack and maybe even lose your computer. But there some straightforward guidelines that should help you protect yourself.

Many people are searching online for information about COVID-19. But the pandemic has created what the World Health Organization (WHO) calls an "infodemic, in which people are bombarded with an overabundance of both accurate and inaccurate information that is circulating on the internet, making it hard to know what to trust.

Hackers have started to capitalize on this situation by sending out emails that purport to offer health advice from reputable organizations such as governments and the WHO but that are really phishing attacks.

It's hard to know how many attacks are being carried out or how many people are being affected. But new attacks are being reported nearly every day, and some cyber security companies are reporting large increases in inquiries since many people started working from home.

One of the first such attacks was reported in Mongolia and was aimed at public sector employees. It involved an email and word document (RTF file) about the prevalence of new coronavirus infections, pretending to be from the country's Ministry of Foreign Affairs. The email and document look authentic and provide relevant information. But opening the file installs a malicious piece of code on the victim's computer that runs every time they open their word processing application (for example Microsoft Word).

The malicious code allowed another computer, known as the command and control centre, to remotely access and control the victim's device, uploading more instructions and malicious software. The hackers can then spy on the affected machine, using it to steal data or direct further attacks.

The pandemic is also worsening the situation because more and more people are staying at home and using the internet to work and socialise. This means they may be using their personal computers more and working outside the normal security protections provided by their employers' internal computer systems. They are also working in stressful conditions that could leave them more likely to forget routine security procedures and fall victim to a phishing attack.

Vulnerable at home

If your computer were to become infected, hackers might be able to steal not only your personal information but also data about your work. And if your device were to crash as a result, you would no longer be able to use it for browsing or remote working. And it might be much harder to get it repaired due to the movement restrictions imposed due to the pandemic.

Luckily, there are some simple things you can do to spot and deal with phishing attacks. Most simply, you can check for obvious signs of fake or unofficial emails such as poor spelling, grammar and punctuation, as most of these emails are generated from outside the country they are sent to. But also be wary if the email tries to create a sense of urgency, that you must click its link now. And if the content seems too good to be true then it probably is.

You should also bear in mind that cyber criminals use every opportunity available to exploit weaknesses in cyber security. And a frantic search for health advice is such an opportunity. So you should always make sure that you look for information about COVID-19 on trusted sources such as WHO.in or theconversation.com.

This article is republished from The Conversation under a Creative Commons license. Read the original article.