# Cyber hygiene keeps your email safe from virtual viruses

March 18 2020, by John Toon



Credit: CC0 Public Domain

The email is from someone you think is a co-worker in another department at your company, who like you, has suddenly found herself teleworking from home without the usual group of colleagues to help review things. She's asking your advice on a document attached to the email.

Being the helpful person that you are, you should just open up that file and give it a look, right? Wrong, says Brendan Saltaformaggio, a cybersecurity expert and assistant professor in the Georgia Tech School of Electrical and Computer Engineering.

Cyber criminals are taking advantage of the fact that more of us are working from home, away from the online safeguards we may have at work. What appears to be an email from a colleague in another department could be an attack that tricks recipients into opening attachments and silently installs malware.

"People will be doing a lot more over email when they work from home," Saltaformaggio noted. "They will be corresponding more with co-workers, sending potentially sensitive documents and interacting with people they may not necessarily know using computer systems that may not have been intended for secure use. That increases risk."

To stay safe from viruses and other malware, Saltaformaggio offers five tips for dealing with email while teleworking under these special conditions—and during the normal office conditions that we hope to resume soon.

- Don't click links in emails when you don't know the sender. Malicious links are among the most common sources of malware. Always hover over a link to be shown the website it links to. Be sure it is the website you expect before you click.
- Double-check before you open files that get emailed to you, especially if they are unexpected. If anything about that email looks suspicious, don't hesitate to call up the sender and ask if they have really just sent you a file.
- When attaching files to email, always double check who you're sending it to. One small typo could send sensitive information to a stranger.

- Watch out for phishing! If something asks for your username and password, don't hesitate to call up your IT people and ask whether that request is legitimate. Your [network administrator](#) won't send you an email asking to you to log into a strange website.
- Thought you had avoided traffic by working at home? Networks can get overloaded when everyone is teleworking. Teleworking spouses and children streaming movies can quickly jam a home internet connection. If everything seems clear on your end, report excessive slowdowns to your IT department.

"Teleworking can help companies get their staffs safely through this crisis, but we all need to be careful to practice good cyber hygiene, just as we are washing our hands to avoid an infection from viruses in the physical world," Saltaformaggio said.

Provided by Georgia Institute of Technology