Working from home during the coronavirus pandemic creates new cybersecurity threats

April 10 2020, by Aaron Mauro

Shelter-in-place directives mean that more and more people are working remotely from home, producing more technological vulnerabilities. Credit: Mimi Thian/Unsplash

COVID-19 has changed nearly every aspect of our daily lives, including how we shop, socialize, exercise and work. If you are a front-line worker or working from home, you must also consider how these adaptations will present opportunities for criminals wanting to exploit this crisis.

In the coming months, many of us will be subject to a range of

cybersecurity threats, such as all-too-common phishing attacks. Public awareness is needed to protect the digital infrastructure of institutions, businesses and organizations of all kinds, including our hospitals and public health facilities. Cybersecurity threats are moving very quickly during the COVID-19 pandemic, and this poses unique problems for mitigating such risks.

As an assistant professor of digital media in the Centre for Digital Humanities at Brock University, I research the historical, ethical and even literary issues related to living a secure life online. I also teach on topics relating to application security and social engineering.

Working remotely—and securely

Cybersecurity is a human problem: the person at the screen or keyboard is always the weakest point in any technical system. Attackers will use a set of techniques—broadly described as social engineering—to trick us into divulging sensitive information.

Just as we have learned to reduce the risk of the coronavirus through social distancing measures and proper hand washing, we will need to develop good security habits to reduce these security risks. After all, we are in the midst of the largest work-from-home experiment in history.

Microsoft's cloud services reported a 775 percent increase in demand across their platforms when strict social isolation measures were put in place.

This situation also presents opportunities for cybercriminals. Attackers have real opportunities to take advantage of the changes in our habits as we transition to working remotely, but there are several best practices that will mitigate the increased risks. The Electronic Frontier Foundation has published some useful guidelines for working remotely.

Security habits

Phishing campaigns use email or instant messaging to coerce a user into inadvertently helping an attacker by clicking a misdirected link, downloading a malicious file or entering log-in credentials.

To thwart such attempts, click on the sender's name and confirm that their name matches the email that you have on record. If you are clicking a link for work purposes, check the link address before you click by hovering over it. Most browsers will display the address on the bottom left corner. You can test this feature by hovering over this link to example.com.

Rather than sending files over email, use a shared file system set up by your employer, such as DropBox, Box or OneDrive. If you have any questions about a file or a link, check with a co-worker or your IT security department.

Avoid opening attachments from email or messaging services. Some of these are known to have experienced security breaches: for example, WhatsApp, Messenger or iMessage.

Your contact information may be easily available online and the speed of instant messaging communications allows for rapid, unintended clicks to compromise your system, often by uploading malware. Slow down the pace of communications to ensure that the people we communicate with are authentic. Be cautious and reflect on the legitimacy of all your communications.

Protecting health-care organizations

A ransomware attack uses a piece of software that locks legitimate users

out of a computer system by encrypting files and demands payment to regain access to the affected system. At present, operators of two large ransomware tools, Maze and DoppelPaymer, have promised to reduce the impact of their scams on critical health-care infrastructure.

Public health organizations and national media from around the world have been asked to entertain worst-case scenarios as a result of COVID-19. An example of a worst-case cybersecurity situation during a pandemic is a ransomware attack against hospitals. The U.S. Department of Health and Human Services published a report in 2016 on ransomware attacks to prepare health-care workers.

Ransomware has been an increasing problem before COVID-19 and the current emergency will only exacerbate the situation.

There has been a recent trend toward using ransomware in smaller municipalities throughout France and in larger metropolitan centres like Johannesburg, South Africa, and Baltimore, Md.., Albany, N.Y., and Atlanta, Ga., in the U.S.

Ransomware has been used against organizations like hospitals and airports, most notably the 2017 WannaCry ransomware attack of the National Health Service in the United Kingdom. Canada has also seen similar increases in ransomware attacks.

Hospitals and other critical infrastructure are at risk of being targeted during the peak of the crisis, where government and public health officials will be exhausted by constant communications. For example, a phishing campaign directed against hospital or public health officials promising personal protective equipment has the potential to cripple some portion of the digital infrastructure that supports our health-care system.

Should a ransomware attack happen in such a situation, it would be logical for an administrator to simply pay a ransom and continue saving lives, which would only encourage future attacks.

Increasing vigilance

We must be vigilant not to spread COVID-19, and we also need vigilance in protecting our digital infrastructure. All institutions, including hospitals and public health organizations, should have recent back-ups that would allow them to rapidly restore services in the event of a ransomware attack.

COVID-19 represents an opportunity to build better digital infrastructure that includes multiple points of authentication, such as two-factor authentication through text message or by mobile app, by default. This more resilient digital infrastructure should also include systems that do not trust each other, so attackers are unable to move horizontally through organizational infrastructure.

While this is no simple task, so-called "zero trust" architecture and multi-factor authentication will increasingly become standard practice throughout institutions, both large and small.

We must be ready to have a public conversation about the legal, technical and personal dimensions of the cybersecurity threats we will face during the COVID-19 pandemic, but we must first be equipped with the questions and issues that emerge from working online in the coming years.

Provided by The Conversation