Lowndes

Five Cybersecurity Practices to Minimize Risk During Coronavirus

Drew Sorrell

Mar 13, 2020

By: Drew Sorrell

As concerns about the coronavirus (COVID-19) continue to grow, many companies are planning to have more employees work from home. While these measures are aimed at keeping employees healthy and safe, it´s also important to keep your organization´s data safe through effective cybersecurity practices.

1. Beware of hackers using coronavirus malware to infect your computer.

Email inboxes are being inundated with messages related to the COVID-19 outbreak from companies, organizations, and government entities. Unfortunately, hackers have seized on this flurry of emails and fear of the pandemic, launching attacks through malware and ransomware. One particular form of attack is malware posing as coronavirus maps and dashboards that infect computers to steal data and passwords.

To protect your work computer, home computer, and digital assistants (including your phone), be extremely cautious before opening a file, clicking a link, or visiting a website that claims to track the coronavirus. These all may be malware vectors. If

you really do need this type of information, access it directly from a trusted source, such as the Centers for Disease Control and Prevention (CDC) or the World Health Organization (WHO).

2. Revisit your wire transfer policies and procedures.

If your organization does implement remote working for employees, revisit your organization´s wire transfer policies and procedure. In addition to communicating this information internally, be sure to notify organizations that routinely send you money transfers (e.g. wires, ACH and so on). The message could state, "ABC Company´s employees will be working from home. Please understand that our company will not be changing its wire transfer instructions. If you receive an email or similar communication otherwise, please call your routine contact at their known number at ABC Company before making any changes. We do not intend to change any instructions." When you communicate pay procedures, communicate about negative policies, too. For instance, "We do not use wire transfers/PCH payments, so if you receive a request for payment claiming to be from us, it is fraudulent."

If changes do need to be made to your wire transfer procedure, a phone call should be made to the other party. Both parties in a transfer are responsible for establishing and communicating policies to help reduce the risk of wire fraud.

3. Implement multifactor authentication for remote working.

With employees working from remote locations, you want to ensure that users accessing the system are actually employees, and not criminals. Multifactor authentication is one way to achieve this. Even if your company doesn´t currently have this deployed, it may make sense to begin this process now given the potential longer-term effects of coronavirus. Multifactor authentication is a best practice regardless of the coronavirus.

Other options for authenticating users include "white listing" or "geo-fencing." White listing only allows "known" computers network access, while geo-fencing only permits computers within certain geographic areas to connect. No authentication approach is perfect, with each offering a different level of effectiveness for your system. The different approaches available should be discussed with your IT leadership to determine the best fit for your needs. Both white listing and geo-fencing are parts of a layered security approach, with layering being a best practice.

4. Encrypt laptops to minimize the risks of loss or theft.

One of the most common forms of data breach results from the loss or theft of a laptop. Laptops should only be deployed with full-disk encryption, which can only be achieved through hardware (i.e. the laptop disk itself has it built-in) or software methods. There are software packages currently on the market that can be installed to encrypt laptop disks.

A word to the wise: be careful installing the software so that you do not inadvertently

encrypt the entire disk, including the operating system. Consult the software installation instructions and your IT professional to avoid this issue.

5. Reduce the cost of an attack with cyber insurance.

While policies and practices can reduce the risk of cyber-attacks and breaches, they cannot completely eliminate cyber-threats. Now is a great time to understand whether your cyber insurance policy and/or crime policy provides coverage for the types of cyber-loss that may arise during remote working (including ransomware, social engineering fraud, data breach and the like). If you don´t have a cyber-policy and/or a crime policy, now would be a good time to start working on obtaining one.

For up-to-date news please follow our Coronavirus (COVID-19) Response Team page.