Is That PC Safe? – How to Quickly Deploy New PCs to Support Your COVD-19 Telework and Telehealth Efforts

By Mitch Parker, Chief Information Security Officer, Indiana University Health, in collaboration with John Riggi, AHA Senior Advisor for Cybersecurity and Risk.
March 23, 2020

The Department of Health and Human Services issued an alert on March 21 that some new, off the shelf PCs, from a major online retailer were found to have embedded malware.

This may be an emergent situation impacting risk to new PCs and other computer peripherals from where you will be picking up PCs to support the business. You may not have the advantages of programs such as Dell ImageDirect, if picking up used or refurbished PCs due to supply chain issues.

Here are some tips to make sure the PCs and laptops you deploy quickly are as secure as possible and reduce the risk of malware. We realize these tips are not all inclusive, but hope they serve as an option for a convenient, quick start reference guide.

Recommended Steps:
- Be wary of the firmware: For each of the PCs you deploy, get the latest firmware from the web site. Both refurbishers and sellers of new hardware don't always deploy the latest. With the critical Intel and AMD vulnerabilities out there, you need to deploy the latest firmware. These can mitigate critical firmware and management level vulnerabilities.
  - If you purchased new or refurbished Dell PCs, you can even do this without booting into Windows:
    - [Flashing the BIOS from the F12 one-time boot menu](#)
    - Create a bootable flash drive using the Dell Diagnostic Deployment Package (DDDP) using instructions [here](#) and then follow step #7 [here](#) to copy the BIOS update to it and run it.
  - If you purchased a Lenovo you can make a bootable flash drive by following instructions [here](#)
  - If you purchased an HP you can make one by following [these instructions](#)
- Don't trust the image or software on there! Especially if you bought a used PC, there may be malware on it from the last owner. Don't use the operating system software that came with it.
  - Use your image whenever possible for a PC or laptop and keep it updated!
  - If you don't have an image, you can get a fresh copy of Windows 10 [here](#) to do a fresh operating system install and reformat the drives.
  - If you need Microsoft Office, you can do an offline install [here](#).
  - Make sure Automatic Updates are turned on!

- If you don't have a program to mass install images, an option is [Clonezilla,](#) to build images you can use to rapidly deploy your master image to your new PCs to save time. You can find a tutorial [here](#).
- For endpoint protection, Windows Defender or one of the endpoint detection and response tools such as Cylance, Crowdstrike, Proofpoint, Elastic Endgame, or Cybereason among others, should meet your needs and provide sufficient performance, even on refurbished hardware!