The Security Risks of Using Preowned Hardware

Introduction

There is often the view that if you purchase preowned hardware (especially from a third party), that it is not as good as buying it directly from the vendor. However, as one of our previous blogs have examined, buying preowned hardware is just as good, if not better, than getting it straight from the source. But just like anything else, there can be security risks involved. In this blog, we examine those risks and provide tips as to how you can mitigate them.

The Top Security Risks

1) Keylogging software may be installed:

   Keyloggers are software packages that can be deployed on just about any computer, server, or wireless device. The intention of this is to secretly record what you are typing, which is then transmitted back to the previous hardware owner. Keyloggers can be very difficult to detect.

2) Malware could be present:

   This is a more advanced version of a Keylogger. For example, it can record your web browsing history, install cookies without your consent, and even search your computer for other types of personal information that you may have stored on the hard drive. In more extreme cases, it can even view your presence through the webcam.

3) It could be the target for Cryptojacking:

   Cryptomining software typically mines for the virtual currencies, such as Bitcoin, etc. However, this requires more processing power and electrical consumption on part of your preowned hardware. Thus, it could be the case that the seller has actually installed this onto your hardware, so that they can illegally mine for these currencies (which is technically known as "Cryptojacking"). The tell-tale signs of this include slower than normal speeds when using your computer or wireless device.

4) Deleted files can still be lurking:

   When you delete a file from your computer, there are still traces of it in your hard drive. For example, although you may not see that file anymore where it was originally stored, it is still in your system. All that deleting does is simply mark that specific file so that it can be overwritten with a brand new one. Worst yet, these deleted files could even contain some sort of malware (such as a Trojan Horse) that can be secretly launched when you turn on your preowned hardware for the first time.

How to Mitigate the Risks of Preowned Hardware

Here are some tips to make sure that you stay safe:

1) Wipe the hard drive clean:

   Before you actually start creating and storing files, make sure that you have wiped out the hard drive just after you purchase your preowned hardware. This is often referred to as "nuking",

and there are many tools available that can help you accomplish this task. Not only will any existing files be completed flushed out, but any "junk" data as well.

2) Replace the hard drive:

   If for some reason you are unable to "nuke" the hard drive, then the next best option would be to replace it in its entirety. But you have to make sure that you can actually procure this from a reliable source. This all depends on how old your preowned hardware is. The older it is, the more difficult it will be to find the right hard drive.

3) Make sure that the BIOS is updated:

   Always check for the latest updates as it relates to the BIOS. Make sure that you download and install the latest version, in order to get rid of any surprises that could still be lurking in the preowned hardware. This process is known as "flashing the BIOS".

Tips to Make Sure That You Avoid These Security Risks

1) Make sure that the pre-owned hardware has been 100% refurbished to factory specs:

   The hardware needs to have the most updated versions of both firmware and software. It also must be tested to ensure that it is operating within the appropriate specifications. Make sure that it is certified as well.

2) Make sure that you have the same warranty plans in place:

   You need to double check that the preowned hardware that you are about to purchase is backed by the same warranty plan as the manufacturer offers. In addition to this, you also need to make sure that you have the equivalent support and maintenance plans as well. If this is not in place, you could potentially lose a lot of money if the equipment does not work properly.

3) There are no hidden costs:

   You should be paying the retail price and nothing more. Be wary of any hidden and inflated costs. If there are any, these should be a red flag to you. Also, be aware of any products in which the "prices are too good to be true". There could be defects with them, and could even pose a grave security risk to your company.

4) Confirm that the reseller is certified by the OEM:

   While the prices might be much cheaper at eBay or Amazon, there is no guarantee that the product you are getting has been tested, or even has a warranty plan with it. You should always procure your hardware from an authorized reseller, and one that has been certified by the OEM. That way you are assured that you are buying the real thing.

Conclusions

PivIT believes, you—as the customer—deserves options when it comes to your preowned hardware, maintenance options, and warranty plans. OEM's would love for the customer to believe you need to purchase and install new equipment every 2-4 years. However, at PivIT we are passionate about

empowering the customer with knowledge and options to know which preowned equipment to purchase.

Most businesses don't realize that with proper maintenance options (like our Lifetime Warranty or OneCall NBD or 4HR support options), preowned hardware can easily last 5-10 years, if not longer. Nothing makes us more satisfied than knowing we are helping businesses save tens of thousands of dollars by helping them understand their different options when it comes to using new versus legacy equipment.

At PivIT, we are 100% OEM certified, and all of the preowned hardware that we sell to you conforms to the standards as set forth by the vendor. You can be rest assured that they have the latest firmware and software upgrades installed onto them.

Do you need help in learning which preowned hardware you need? Do you have questions or need further guidance? PivIT Global has a wide variety of product offerings to meet your needs and everything in between. Reach out to us with your questions at hello@pivitglobal.com or 1-888-747-4847.

Sources

1) https://security.stackexchange.com/questions/198398/what-are-the-risks-of-buying-a-used-refurbished-computer-how-can-i-mitigate-tho
2) https://www.makeuseof.com/tag/risks-buying-used-pc/
3) https://www.networkworld.com/article/2159650/top-things-to-consider-when-buying-pre-owned-equipment---a-buyers-guide.html