INSIGHT SERIES

Business Computer Selection & Best Practices

Feb 1, 2022

www.fcicyber.com

Table of Contents

1 Introduction

When selecting a computer to be used for business it is important to know that a business computer can be used for personal reasons, but a personal computer should never be used to conduct secure business.

2 Home vs Business Computers

Personal computers are outfitted with a “Home” version operating system (OS) and functionality limitations, which is why they are more affordable. Though satisfactory for general purpose use, personal computers are not configured with business-grade functionality required to meet business standards. For example, personal computers do not enable structuring personal and business data separately, which results in data comingling and presents security vulnerability.

To further illustrate this, a Windows 10 Home computer linked to a personal Microsoft Live account cannot simultaneously link to a business account necessary for automated, professional cybersecurity.

Professional, business-grade computers feature sophisticated functionality that enables high level performance, especially related to cybersecurity safeguards. The dedicated use of a business-grade computer running the most up to date professional version software is best practice. An advantage in opting for a business-grade computer is that any personal activity will also be as secure as possible.

Upon selection of a business computer, promptly install professional grade cybersecurity software to safeguard the system and the private data it will contain.

Dedicated use of a business-grade computer running the most up to date professional version software is best practice.

3 Computer Variables

Computers consist of varied components including device features and functions as well as operating system (OS) edition, version and build number. It's important to become familiar with the specific build of your machine and its lifecycle requirements.

To locate device specifications:

- For Windows: type "About" in the search bar
- For Apple: choose Apple menu > About This Mac

All computers are configured differently.

4 Lifecycle Management

Important Note: If you are supported by an IT professional, your machine may be managed on your behalf in accordance with firm policies and any changes should be discussed.

4.1 Cybersecurity

Managed Endpoint Security is crucial. As a best practice and to meet regulation compliance, devices that access non-public information (NPI) require tracking and management from the time acquired until destruction.

In response to a Presidential Executive Order,[1] the National Institute of Standards and Technology (NIST) developed cybersecurity framework[2] that includes Identification, Protection, Detection, Response & Recovery guidance to help organizations manage risk.

Professional cybersecurity technical controls that meet NIST criteria should be installed on every computer that accesses NPI and an Asset Inventory Report that includes a list of all

[1] EO 13636 (Feb 2013), Improving Critical Infrastructure Cybersecurity
[2] NIST Cybersecurity Framework

computers and their cyber posture should be utilized for logging, monitoring and quality control of digital assets.

If the endpoint is not secure, nothing is.

4.2 System Updates

System Updates deliver critical security, software, and feature improvements to keep your system at the highest level of protection and performance. As a best practice and as required by some regulations, your OS and antivirus should be maintained as the latest, most secure, version available. Additionally, all applications should be updated regularly.

Timeliness of system update installation matters! As soon as a system update is available, the best practice is to immediately allow or schedule your machine to install it promptly.

4.2.1 Reboot Is Required

To trigger software update installation, you must "Restart" your computer. System restart, also called "Reboot" is required to install system updates and is not the same action as shut down or sleep mode.

- Restart completely ends all processes and reboots the machine freshly
- Shut down powers down processes and creates a hibernation file that the PC later leverages for fast startup
- Sleep mode simply resumes operation where it left off

Note: For MAC, "Restart" and "Shut down" are identical in that processes, cache, and memory are cleared completely refreshing the system.

To ensure most up to date cybersecurity for clients, FCI "forces system reboot or restart" for all users.

System "Restart" is required to trigger update installation. Restart promptly!

4.3 Benefits of Restarting Your Computer

Proper system shut down and restart effects everyone on all devices. The best practice is to log off systems and restart your computer daily. While developing this good habit does require effort, routinely restarting your system improves security and performance:

- System updates, including critical security improvements, are triggered to install
- System values are cleared (RAM, CPU, temp files) allowing the device to start anew
- Improved performance
    - Leaving everything running means your computer doesn't have the opportunity to refresh, which results in glitches and crashes
- Increased speed: an efficient system provides faster operation
- Can correct connectivity problems (network drives, internet, Wi-Fi)
- Can correct hardware or driver functions
- Halts memory leakage

Helpful hint: "Have you tried restarting your computer?" is a famous question for good reason.

4.4 Software Update vs Upgrade

Software update and upgrade are two different ways to change your operating system (OS).

An update consists of critical security fixes to remain up to date as well as system/feature improvements. Updates are typically free of charge as they modify a pre-existing installation.

An upgrade replaces the software version, improving your OS to a higher standard. Upgrades come at a cost (sometimes discounted based on previously existing version) because an upgrade is considered a new product.

Software updates are necessary whereas upgrades are generally not— until a product is approaching "end of service life" and will no longer be supported with critical security updates. When a machine is no longer updated with critical security updates it becomes at risk (and out of regulatory compliance).

4.5 Password Management

To protect access to private data, strengthen your credentials by using a Password Manager to securely store them. Password data is robustly encrypted to your device and safeguarded in a protected vault further secured by Multi-Factor Authentication (MFA).

A Password Manager app offers ideal balance between security and time-saving access. It eliminates risk of weak and reused passwords and enables complex password generation.

Create a strong master password that you can memorize because it will be the only one you need. Remember to never allow your browser to save your passwords since they are easily accessible to hackers.

4.6 Routine Maintenance

Routine maintenance and good physical care help a computer to perform optimally.

- Dust regularly
- Use a surge protector
- No liquid/food near machine
- Keep pets away
- Avoid extreme temperatures
- Charge laptop battery then power down and unplug
- Delete extra files/apps
- Defragment Hard Drive
- Run Disk Cleanup
- Disable Unused Programs

4.7 Regular Backup

Refer to your agency/firm established guidelines for backup procedures.

Data backup should be performed regularly to preserve files in the event of a system failure. External hard drives are a popular choice for backing up as well as software-based backup, which allows for going back in your timeline in case of a glitch. Best practice is to determine a backup schedule and adhere to it strictly.

4.8 End of Service Life

Like all products, devices and software become outdated. Manufacturers determine product lifecycles based on demand, technology advances and cost affiliated with support. It is important to be aware of the lifecycle requirements of your computer as well as plan for required action at the End of Service Life (EOSL).

In accordance with manufacturer policy, OS software has a determined lifecycle, during which, critical security updates are provided. As an OS approaches EOSL, an expiration date is set for remaining updates and beyond that date the product is no longer serviced—or secure.

It is imperative for security (and performance) to maintain up-to-date systems. Act to keep your system current before critical security updates stop being published for products nearing EOSL. Depending existing OS version, you may be able to update to a supported version or it may be necessary to upgrade to a newer OS version.

Those with malicious intent lie in wait for systems to become vulnerable once they are no longer updated. You may believe you are protected and compliant because you are receiving updates but if you are no longer receiving "critical security'" updates, your computer is at risk as well as out of compliance. Critical security updates only happen if they are available for the OS version you are running. Best practice is to review the contents of system updates to ensure your computer is being updated with critical security improvements.

When evaluating device upgrade, be aware that as a computer ages it may become difficult to install new programs or OS upgrades due to software/hardware incompatibilities. Plan for computer replacement in advance to avoid compelled action due to aged hardware.

If you are no longer receiving "critical security" updates, your computer is at risk as well as out of compliance.

4.9 Decommissioning

As a best practice and to meet compliance requirements adhere to a proper procedure for computer decommissioning that includes evidence preservation.

Every computer that has accessed NPI requires proper decommissioning when it will no longer be used. When preparing for discontinuation of a computer, you must properly erase

all private data and document the process of decommissioning, including evidence of computer destruction or repurposing.

Proper decommission of a machine that accessed NPI includes:

- Erasure of all NPI
- Written attestation of NPI removal
- Evidence of hard drive encryption before destruction
- Removal of cybersecurity tools
- Documented destruction of hard drive
    - Destruction certificate from a third-party vendor
    - Picture evidence of destruction
- If repurposing, evidence of hard drive wipe
- Follow local requirements for electronics disposal

To help clients, FCI offers a decommissioning process for devices that contained NPI.

5 Key Takeaways

- Dedicated use of a business-grade computer running most up to date pro version software is best practice.

- An advantage in opting for a business-grade computer is that any personal activity will also be as secure as possible.

- Become familiar with the specific build of your computer and its lifecycle requirements.

- Devices that access NPI require tracking and management from the time acquired until proper destruction.

- An Asset Inventory Report should be utilized for logging and monitoring digital assets for quality control.

- As a best practice and as required by some regulations your OS and antivirus should be maintained as the latest, most secure, version available.

- Install “system updates” as soon as available. Updates contain critical security improvements to keep your system at the highest level of protection. To trigger update installation, you must “restart” your computer.

- Best practice is to log off systems and restart your computer daily.

- It is imperative for security (and performance) to maintain up-to-date systems. Act to keep your system current before critical security updates stop being published for products nearing End of Service Life (EOSL).

- When a computer no longer receives critical security updates it becomes at risk (and out of regulatory compliance). Critical security updates only happen IF they are available for the OS version you are running.

- Adhere to a proper procedure for computer decommissioning that includes evidence preservation.