The Secure Image and You: FAQs for Those New to Computer Security

Question #1: What is a “secure image”?

A secure image is not really a computer image in the traditional sense. A computer image is a complete package of an operating system, applications, and settings that is standardized for a business. A secure image is actually an additional package of applications and security settings added to our standard computer image that you all know and love. The security is to help prevent and/or reduce malicious virus attacks, snooper programs, and uninvited users and hackers from having free reign over your computer system and its precious cargo ……your data.

Question #2: What’s different between a standard image and a secure image?

Not a lot. The average user who gets the secure image still receives the same suite of software that someone with the standard image receives. The secure image just has a number of security settings, security applications, security protocols, and security restrictions that makes it really hard for outside forces to access your data. Most of these protections people will never notice.

It sounds scary but it really isn’t. It just takes getting used to. Here is a list of the primary changes, reasons behind them, and how they may affect you and your computer etiquette:

• **It’s time to say goodbye to default administrative privileges**: Users will no longer be granted default administrative rights to their computer. It’s hard to let go of an old friend, but there is a good reason behind it. Viruses, Trojans, and rootkits can attack you from almost anywhere nowadays. From a fake or spoofed website or email to an ad that is auto loaded when you connect to a search engine, they are out to get you and your information. By running daily from an account with admin rights, you are giving all of them permission to have access to every part of your system. 90% of people’s work can operate just fine as a standard user. The rest will have special configurations made to allow the user to work even without admin rights.

• **BitLocker, data encryption for everyone**: You’ll notice when you first turn on your machine that you will be required to put in a 6 to 15 character numerical pin code. That’s BitLocker hard at work for you. It encrypts (equivalent to padlocking) the data on your main drive making sure that anyone who doesn’t have a key to access can’t access the data on that drive. Why, you ask? Because if your machine (especially in the case of laptops) gets stolen, misplaced, or mishandled, anyone can pull that hard drive out and pull the data off.
Critical University information would be exposed, risks of lawsuits could be lingering overhead, etc. The initial encryption may take 2-4 hours; but afterwards, you will hardly notice it.

- **Bit9 Parity, do you really need that app on your machine?** Adding to the security suite is Bit9. This software restricts random, unplanned, and unapproved applications on your machine. Do not fret. All Division of IT standard applications are pre-approved, as well as are many business-related applications. The key here is to prevent random applications like toolbars and ride-a-long apps from installing and running on your machine. Did you know viruses and Trojans may try to install applications to steal your information without you knowing, and they can ride-along on freeware applications from instant messaged ads to P2P networking clients to desktop background apps? You can speak to us about whether your app will be allowed through Bit9.

- **Additional group policy settings, will they interfere with your work?** The answer for 95% of situations... No. These group policy changes mostly affect data transmission security, aka, how your data is moved about on the network. They should be transparent and seamlessly fit onto your machine. There is no 100% certainty for these and they will be adjusted on a case- per-case basis.

- **Msuitadmin account will be disabled, early retirement:** We usually keep a local admin account for maintenance purposes. We'll be disabling that account. Why? Accountability. You see, that account is considered to be a generic account. A generic account is one that officially does not belong to one person but is shared to several. We're switching to a process where all admin rights are centrally managed and where all changes on a machine are tracked. This way we can see who worked on your machine last and what they did. This will help better address situations in dealing with your computer.

- **A priority max security package, for locking down critical data machines:** There are computers out there that handle very sensitive data which will need even more protection than was stated before. These machines will only get the bare essential applications from our standard app collection, as well as user access restrictions and additional group policy settings.

**Question #3: Do I really need this “secure image”?**

If you are constantly working with student information accessing a Social Security number or key personal information, then, Yes. If you are dealing with key financial information within this University, then, Yes. If any data on your machine could compromise this University, then, Yes.

*We're taking data security very serious and so should you.*