The Secure Image and You: A FAQ for those new to Computer Security

Question #1: What is the Secure Image?

The “Secure Image” is not really a computer image in the traditional sense. A Computer image is a complete package of Operating System, Applications, and settings that is standardized for a business. The “Secure Image” is actually an additional package of applications and security settings to our standard computer image that you all know and love. The security is there to help prevent and/or reduce malicious virus attacks, snooper programs, and uninvited users and hackers from having free reign over your computer systems 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 the protections most people will never notice.

It sound 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 Root Kits 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? If your machine (especially in the case of laptops) get 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 now lingering overhead, etc. The initial encryption may take 2-4 hours but afterwards, you will hardly notice it.

- **Laptop Lids:** Speaking of laptops and the security of data, did you know that it’s very important that if you are using your laptop on a secured image and you are not plugged to power and close your laptop lid your machine will shut down? This safety feature is essential to the bullet point
above and ensuring that in the case that a laptop should be lost, stolen or otherwise that it’s
data be protected from those that may mishandle that data.

- **Bit9 Parity, do you really need this application 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 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 long freeware applications from instant messenger 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 seamless fit onto your machine. There is no 100% certainty for these and they will be adjusted on a case per case basis.

- **Priority Max Security Package, Locking down critical data machines:** There are computers out there which 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 personal information with a social security number or key personal information, then yes. If you are dealing with key financial information in dealing with this university, than yes. If any data on your machine could compromise this University, then, yes.

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