What is a Content Management Site (cms)? Unlike a static website, the ESSIC cms builds page views when a user requests the page. The ESSIC cms is a group of related databases and data tables that contain the content and web pages that request information from the data structure. This type of arrangement allows the ESSIC cms to be updated ‘on the fly’ without causing disruptions of service.

This structure allows users to update their own profiles with many different types of information. The cms structure eases updating with fresh content, since updating sections is seamless to the user and requires no programming experience by the content managers.

The new site also includes an updating and expanding outreach section. There are blogs written by the faculty, spotlight articles and in-the-news features. The spotlight articles and in-the-news features are written by the Web Journalism staff at m-square. These are recently graduated or rising journalism students from UMD.

The new site has dynamic modern features that help bring focus and attention to the ESSIC research.

Are you marketing yourself and research effectively?

Google your name and ESSIC. Your ESSIC profile will most likely appear on the first page of results. Go to your profile and see if it is filled out completely. Part of the new cms site (see article above) allows new users to create robust personal profiles.

The site was developed to take advantage of web search sites to place profiles in high visibility spots on search returns. If you need help with the login process, go to login help page on the ESSIC site.
DNS Changer Malware

The DNS Changer malware is a virus that altered DNS settings to redirect web queries to harmful DNS centers. DNS stands for Domain Name System. The DNS server takes the information you type into a web browser and translates it into an ip address based on the internal database. The DNS resolver is the client side of this interaction.

The DNS changer malware gets between this exchange and redirects individual machines to harmful DNS servers that may contain a large amount of harmful malware. Since this interaction between the DNS server and resolver is mostly allowed it can be very harmful.

The FBI has maintained servers to help protect against this redirection. The FBI servers will be taken offline on July 9th, 2012. Any computers or DNS servers still infected will have web redirection problems. To check if your system is infected go to this link. If the DNS resolution is not green please contact the helpdesk immediately.

Requirements for Computer Purchases

The end of life is near for Windows XP (spring 2014 or sooner) and new systems will be using Windows 7 64-bit. Windows 7 is a robust O/S written for multi-core machines with robust ram and hard drives. The rapidly sinking cost of hardware has also seen a rise in the resources needed by common ESSIC software like Microsoft Office and Matlab.

Due to these reasons ITAP has determined that any new personal computer purchased meet the minimum requirements below:

- 4 gb of RAM
- Dual core 64-bit capable processor
- 2 ghz processor
- 128 gb internal Solid State drive or 250 gb Internal SATA drive

ITAP recommends a 3 year life cycle on personal computers. Desktop systems including monitors can be purchased for under $750 at the time of publication. Servers and group machines are still configured to order depending on the group tasks.

ITAP Inventory Tags

As the faculty and staff size has increased at ESSIC, the need for a more robust inventory tracking system has arisen. Earlier this year, inventory tags (pictured on the left) were installed on all UMD and ESSIC managed IT assets. These tags will help identify which assets ITAP is responsible for maintaining.

On the backend of these tags is a database that includes various pieces of information about each system. ITAP has easy access to hardware and software configurations, assigned users and system locations. By only giving the ESSIC inventory tag number, the helpdesk will have all the information about any particular system. The process has started to include this database into a more modern helpdesk web interface that assigns help tickets and help cuing.
Many of us have received e-mails from scammers that talk of riches in Nigeria if we can send money for processing. In the last newsletter, ITAP issued a list of items to be on the lookout for in scam e-mails. It seems obvious that these e-mails are fraudulent. The question remains, Are these scammers leaving the tell-tale signs of fraud on purpose or are they ignorant?

Microsoft security specialists looked into the issue and have published a fairly detailed explanation of Nigerian scammers (Link). The summary is that to remain profitable, the e-mail scam must eliminate non-viable users and minimize false positives. Basically, they are preying on the most gullible and most ignorant of computer security in society. By making outlandish statements and having easily discernible signs of fraud they can eliminate targets that are a wasted effort.

Pop Up Protocol

What should you do when you get an unexpected pop-up on a website?

First- DON’T PANIC. Try to ascertain if the pop-up could be legitimate. Are you on a data downloading site? Are you trying to view a Quick-Time attachment in an e-mail? These could be legitimate pop-ups. There should be no pop-ups from the security software on ESSIC PCs asking the user to download anything!!!!!!!! Adobe and java downloads should ask permission to install within the first minute of logging into your machine. No sites should ask a user to upgrade their java or flash version in ESSIC.

Second- hit ctrl-alt-delete to bring up the task manager.

Third- kill the browser in the task manager.

Do Not hit the cancel button or x-out of the window. If this is a malware intrusion then the cancel and x-out buttons are probably really the OK buttons. If after you have successfully exited a potential malware pop-up and your PC is not behaving normally contact the IT Helpdesk immediately.

User Account Changes

Due to the growing number of users and pervasiveness of modern malware, ITAP will initiate account user privilege changes ESSIC wide. In a recent Microsoft study 90% of critical windows 7 vulnerabilities are mitigated by using standard user account privileges. These changes will be made to machines released to the user community starting in July 2012. In the next several months, the changes will be made to existing systems. Below is a snapshot of the major stats from the study.

90% of Critical Windows 7 operating system vulnerabilities are mitigated by having users log in as standard users

100% of Microsoft Office vulnerabilities reported in 2009
94% of Internet Explorer and 100% of IE 8 vulnerabilities reported in 2009
64% of all Microsoft vulnerabilities reported in 2009
87% of vulnerabilities categorized as Remote Code Execution vulnerabilities are mitigated by removing administrator rights.
HELPDESK CONTACT INFORMATION

For all your IT questions, problems, etc.

Walk-In   #4061
Phone 301.314.2627
E-mail mmaddox@essic.umd.edu

Online Resources:
http://www.essic.umd.edu/~mmaddox/
ithelpdesk/

http://helpdesk.umd.edu/

Windows 8 Preview

Now that we have installed Windows 7 on 95% of ESSIC machines, Microsoft is introducing Windows 8. The new operating system is designed to take advantage of advances in touch screen computing and allow users to sync their experience through Microsoft SkyDrive to all windows 8 machines. The new system has to interfaces; 1 very tab-
let like interface based on windows phone and the other very windows vista/7 interface. The second interface is only available on x86(Intel, AMD, etc.) chipsets. Tablet ARM chipsets will only have the metro interface similar to windows phone.

ITAP has a dell tablet running windows 8 with the basic ESSIC suite of software. Anyone wishing to get a sneak peak and some time on windows 8 please contact the helpdesk.
ITAP is currently running the UMD VPN agent, ssh client, office2010, Acrobat X and Mozilla. From my short time with the system, it appears to fill the tablet role for users and security needs of ITAP.