MEDICAL GENETICS IT SECURITY AND AWARENESS NEWSLETTER, FEBRUARY 2013

MOBILE DEVICE SECURITY POLICY, IT-12.1

Personal mobile devices are not supported by MMGE IT Staff, but if they are used to access MMGE and IU IT resources, they must be configured securely. The university has adopted policy IT-12.1. The policy defines minimum security standards and also requires users to report a lost or stolen device to the UISO at it-incident@iu.edu . To view the policy in its entirety, please visit https://protect.iu.edu/cybersecurity/policies/IT12/12.1

JAVA ON WORKSTATIONS

Sun's Java virtual machine has seen a spike in actively exploited vulnerabilities, and leading IT security organizations are recommending its removal, or at the very least limiting deployment to areas where absolutely necessary. Vulnerabilities in Java are responsible for a large percentage of "Scareware" and "Fake Anti-Virus" incidents.

Effective March 1, 2013, Java will no longer be pre-installed on new computer installations. If Java is required for a business purpose, it will be installed, configured with the highest possible security settings, and documented to enable a rapid response for future vulnerabilities. Over the next few weeks, older versions of Java will be removed from existing workstations, and you may notice increased overnight reboots while workstations are scanned and patched.

PASSPHRASE EXPIRATION CONTINUES

IU continues to expire passphrases older than two years on a rolling basis. If you are prompted by CAS to change your passphrase, please do so as soon as feasibly possible. Your access to IU resources could be disabled with little warning.

PHISHING SCAMS

Several phishing scams have made the rounds with increasing sophistication and authenticity. Please remember that nobody from IU will ever contact you via email requesting your credentials. It is generally unnecessary to report these types of messages – the best course of action is to simply delete these messages.

E-MAILING PHI

If you need to email PHI or other sensitive information, include the phrase "Secure Message" or "Confidential" in the subject, and it will automatically be encrypted and delivered via the Cisco Registered Envelope Service. Do not rely on the outbound message detection to automatically encrypt your message. Please see https://kb.iu.edu/data/bbtq.html for more information.

VOICEMAIL PHI CONCERNS

If you check your voicemail at home using Outlook Web Access by downloading .WAV files and then playing them with iTunes,it is possible to inadvertently share these messages with other people. Please take the necessary steps to disable iTunes library sharing and configure your computer to play .WAV files using Windows Media Player or another non-Apple media player.

IU.EDU E-MAIL ADDRESS TRANSITION ISSUES

The IU.EDU e-mail address transition had some unforeseen consequences with the Lync phones that have been deployed throughout the department. These issues were reported to the Identity Management team and have been used to enhance documentation and processes elsewhere on the campus to ease the transition for other departments. Most of these local issues have been resolved, but if you continue to have issues with Team Calling or with your sign-in address, please send a trouble ticket to mmgesup@iupui.edu for assistance.