Information Security Ransomware Alert

"CRYPTOLOCKER"

Dear Faculty, Staff, & Students

Albany State University Information Security Office has been made aware of a ransomware (malware) virus called 'CryptoLocker' that is currently infecting Windows computers. We want you to know about the program, what we are doing to protect devices on our network, and how you can help. Although this virus currently affects only Windows devices, Mac users should also be aware of the problem as well.

Information Technology Services (ITS) has proactively deployed countermeasures to protect our Information and Information Systems. As end-users, we can assist by applying the skills learned during our Information Security and Awareness training such as Safe Browsing and SPAM & Phishing avoidance. Remember, YOU ARE THE TARGET!

ITS recommends you be especially careful at home. Home users are at greater risk because they are not trained in Information Security and don't believe they are being targeted! We have included some tips to assist in keeping our ASU family members safe at all times.

KEY INFORMATION:

What is Cryptolocker?

CryptoLocker is malicious software that encrypts your data files (word, powerpoint, pictures, music, videos, etc.). This ransomware will encrypt certain files using a mixture of RSA & AES encryption. When it has finished encrypting your files, it will display a CryptoLocker payment program that prompts you to send a ransom to decrypt the files. Ransoms of up to $3000 have been reported. More Information: http://www.us-cert.gov/ncas/alerts/TA13-309A

What is Encryption?

Encryption encodes your data so only you and authorized people or authorized websites can read the data.

How do I protect my computer?

- Make sure your antivirus is running and is up to date. Many antivirus programs detect the malware. DO NOT postpone or prevent LANDesk from updating your anti-virus software.
- The malicious link may be embedded in emails. Don't click on the links! IF IN DOUBT, delete ANY suspicious email.
- Back up your data! If you have a backup, you'll probably be able to restore the data.
- Report suspicious emails to helpdesk@asurams.edu and/or to infosec@asurams.edu

What if I think my computer is infected?

- Disconnect the computer immediately from ALL networks, wired or wireless.
- Power OFF your computer to prevent any further contamination and Contact the ITS Helpdesk
- If your computer becomes infected you may see the screen below:

Home Computer Use Information and Tips!!!

- Make sure you have Up-To-Date Anti-Virus running on your home computers
- Backup your IMPORTANT files such as tax information, pictures, videos, etc. with an external USB hard drive
- Disconnect your external USB hard drive after backing up information
- Install patches and Windows updates
- Activate your windows firewall
- Practice the same preventative measures at HOME as you do work
- Educate your AT HOME computer users
- Helpful Link: Taking control of **computer security** - **Windows** - Microsoft

Thanks,

Marcel Anthony
Chief Information Security Officer
ITS, Information Security Office