THE UNIVERSITY of MISSISSIPPI
OFFICE OF INTERNAL AUDIT

April 2018 Newsletter

The Audit Perspective

In This Issue

Computer Security

Computers are a necessity to most jobs across the University. Universities retain many types of sensitive information, making them a target for cyber criminals. According to a recent EDUCAUSE article, *Top 10 Issues, 2018: The Remaking of Higher Education*, the #1 issue is information security. Cyber criminals can use your computer for a variety of malicious activities such as:

- Sending out spam
- Hosting malicious websites
- Launching attacks on other computers on the network
- Obtaining user logins and passwords to University systems
- Obtaining personal information of the device owner related to any activities performed on the device (banking, healthcare, etc.)

This issue of our newsletter will discuss basic settings you should have on your computer to help ensure University information is protected. The items discussed in this newsletter are required by the University's Anti-Virus Protection for UM Computers Policy and Information Confidentiality/Security Policy.

To assist you in ensuring you're protected, detailed instructions on how to check and/or setup your computer for the below mentioned security controls are attached here:

- Windows 10
- Mac

Additionally, the IT Helpdesk can be contacted for assistance at (662) 915-5222.

Updating/Patching

Computers should be configured to apply application updates and operating system (OS) patches daily. Most attacks launched by cyber criminals today target known weaknesses and vulnerabilities in your computer. By running the latest version of both your

operating system and applications, you are secure from most known attacks. Most operating systems support automatic updating where the update will automatically download and install which makes it very easy to keep up with the latest OS updates.

Tip: During departmental audits, we frequently find OS updates have not been checked in a very long time. This can be caused by the auto-update feature being turned off.

Anti-Virus Protection

A common method for hacking into your computer is to infect it with viruses, worms, or Trojans. These malicious programs (often called malware) are programs designed to give someone else total control of your computer. This can result in loss of data and inappropriate access to University information. Anti-virus is an effective way to help protect your computer against this threat.

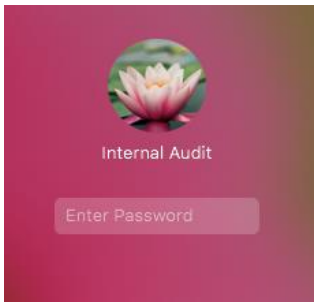
The current recommended anti-virus solution is Symantec. Departments are able to purchase Symantec from the Faculty Technology Development Center's website at a discounted price. Any alternative anti-virus solution must be approved by the Chief Information Officer or Security Coordinator before being used.

Tip: Check your Symantec anti-virus regularly to ensure it is turned on and definitions are up-to-date. During departmental audits, we have found Symantec may be installed, but it is either not turned on or the definitions have not been updated.

Firewalls

Cyber criminals can also hack into your computer through known vulnerabilities via the Internet. Similar to anti-virus, a firewall is a security program designed to protect your computer. A firewall decides which computers can and cannot talk to your computer. Security software usually combines both anti-virus and firewall into a single product, as is the case with the University approved version of Symantec. Additionally, Windows and Mac OS both have firewalls built-in. At least one firewall should be properly configured and enabled in order to protect you.

Screen Password Lock



Employees must use a session/screensaver lock to prevent access to data after a certain period. Session lock is recommended after 15 minutes of inactivity. Employees can set a screen saver to begin after 15 minutes of inactivity, then require log in credentials upon resume.

Reference: University of Colorado Office of Information Security Cyber Security Newsletter – Protecting Your Computer
https://www.cu.edu/ois/ois-cyber-security-newsletters

Additional Policy Requirements

Employees should review the Information Confidentiality/Security Policy and be aware of the following additional policy requirements:

Computer & Server Registry
All computers that contain sensitive information must be registered on the UM System Registry. This allows the Office of Information Technology to more frequently scan your computer for potential vulnerabilities. To register your computer, login to myOleMiss and select UM System Registration under "Technology".

Cloud Storage
Sensitive data should not be stored on externally hosted systems, including cloud based storage systems, without a contract that is fully vetted for compliance with University policies. The University has three cloud storage options for faculty and staff:

- Box
- Google Drive
- Microsoft OneDrive

Each one is accessible with your myOleMiss WebID. In order to use these cloud storage services, employees must follow the Cloud Storage Guidelines.

Need an IT Security Refresher?

The Office of Information Technology provides security awareness training at no-charge to all employees. There are classroom and online options. All employees are encouraged to complete the online training periodically. Those with SAP GUI access are required to complete this training every two years. Some departments may be required to complete this training more frequently.

In the News

- Records of 1,882 University of Virginia patients impacted by security breach
- University of Alaska data breach appears to target tax info

Training with Internal Audit

Lead Your Team:
A section on the Code of Ethics and Conduct is presented by Internal Audit during the Lead Your Team training sessions. Lead Your Team is a three-day program designed to

develop the skills necessary to supervise professionally and effectively. This is a core course highly recommended for employees with supervisory and people management responsibilities. The next Lead Your Team sessions are offered on June 6th, 13th, and 20th. Sign up on the HR website!

Account Reconciliation:

The Office of Internal Audit offers training on account reconciliation. A session is currently scheduled for June 14th, 2018 from 11:00am- 12:00pm at the Law School, Room 1115. In this class, employees will learn how to perform monthly account reconciliations for revenue and expenditures (including payroll) in order to be compliant with the Responsibilities of Signatory Officers Policy. This class is designed for signatory officers as well as other employees who have been delegated the responsibility for reconciling departmental accounts. To register for upcoming sessions, go to our website.

New and Updated Policies

The University of Mississippi Policy Directory is a central location for accessing University policies. Since our last newsletter, the following policies have been implemented or updated:

New Policies:

- Counteroffers
- Faculty Workload Flexibility
- Hybrid Entity (HIPAA)
- Restrictions on Uses and Disclosures of PHI (HIPAA)
- Temporary Injury and Illness
- Uses and Disclosure of PHI for Specialized Government Functions (HIPAA)

Updated Policies:

- Accounting of Disclosures of PHI (HIPAA)
- Information Confidentiality/Security – The Office of Information Technology has made updates to the Platform Security Chart.
- Information Security Management Program (HIPAA)
- Payment of Tuition and Expenses
- Procedure for Filling Support Staff Position Vacancies – The Employment Office only reviews application material for non-exempt (hourly) staff positions.
- Transfer Credit

Self-Assessment

Self-assessment is a valuable tool to help identify internal control deficiencies and assist in departmental management and audit preparation. The self-assessment consists of a series of "yes" or "no" questions. "Yes" indicates adequate controls in an area, while "no" indicates control deficiencies. Additional control related information is provided below each question to aid in resolving control deficiencies. Links to relevant policies are also included for each section. The self-assessment can be accessed here. For questions not addressed in the self-assessment, please feel free to contact us at 662-915-7017 or auditing@olemiss.edu.

We hope you find the information in our newsletters useful. If you have any suggestions, questions, or feedback, please contact us at 662-915-7017 or auditing@olemiss.edu.