

Workstation Security



Workstation Security...

Why should we care?

How prepared am I?

What can we do about it?

Bruce Edwards

Information Security Officer

Phone: 502-852-4363

Email: Bruce.EdwardsJr@Louisville.edu

Workstation Security

Why we should care?



The technological environment has changed and continues to change

- **Human nature**
 - Some will always try to take advantage of a situation.
- **Technology**
 - Allows more damage to be done
 - Allows damage that is done to go undetected for longer...
 - *Imagine stealing a customer and /or patient file 50 years ago vs. now.*

Workstation Security

Why we should care?



Change in environment

- Computers every where *but without* computer security
 - Identify Theft, phishing e-mail
 - Computer viruses, Ad-ware, Spy-ware
 - In the news nearly every day...
 - Scandals and fraud

Result

- Very real increased risk of data loss or breach
 - Government interference - Legislated compliance requirements and/or regulations
-
- **WE can take preventative and/or “corrective” action!**

Workstation Security

How Prepared am I?



- Do I avoid sharing or posting my password?
- Do I refuse to log on to let another user work using my ID?
- Do I treat employee, student and other confidential or proprietary data with which I am entrusted with the care I treat my own personal information?
- Do I log off of the workstation when I leave?
- Do I know that I am accountable for any activity that occurs under my user ID and password?
- Can someone easily remove unencrypted data from our facility?
 - How secure is our facility?
 - Is it locked?
 - Who has access? ...Tailgating

Workstation Security

What can we do about it?



Practice “Safe Computing” by following the University’s Workstation Security Policy and Standards:

“All workstations and other computing devices shall be maintained in an environment and manner so that ***access is reasonably restricted to authorized users.***”

All workstations and other computing devices shall be ***used in a prudent manner*** so that data, system and network integrity is likely to be maintained.

All workstations and other computing device operating systems and other software shall be ***maintained in the most up-to-date and secure manner*** possible.”

Workstation Security

What can we do about it?



University's Workstation Security Standards include:

System Maintenance:

- All computing devices operating systems and other software should be regularly reviewed for security updates, patches and tools and be kept up to date with regards to security.

Physical System Access:

- Every reasonable effort should be made to limit and/or monitor physical access to computing devices to authorized personnel.
- Where appropriate and feasible, the display device of computing devices should be situated such that the opportunities for unauthorized viewing are minimized.

Workstation Security

What can we do about it?



Logical System Access and Security

Passwords

- Use a complex password.

Administrator Account (or privileges)

- A dangerous account in windows due to the system access that comes with it
- The Administrator or its equivalent should not be the active user account
- User accounts should not have administrative privileges unless truly needed for university business
- Administrator account or accounts with administrator rights should only be used when necessary and should have a secure password.

Workstation Security

What can we do about it?



System Time-Out

- Configure to lock after a short period of inactivity and require a user ID and password (or other authentication mechanism) to unlock the machine.

Encryption of data

- *Portable* and/or computing devices not located in a secure area used for personal, proprietary or sensitive information should encrypt this information

Wireless Network Access

- Use the University software and never attach to a network that says it is UofL that does not require this software

Workstation Security

What can we do about it?



Protection from Malicious Software

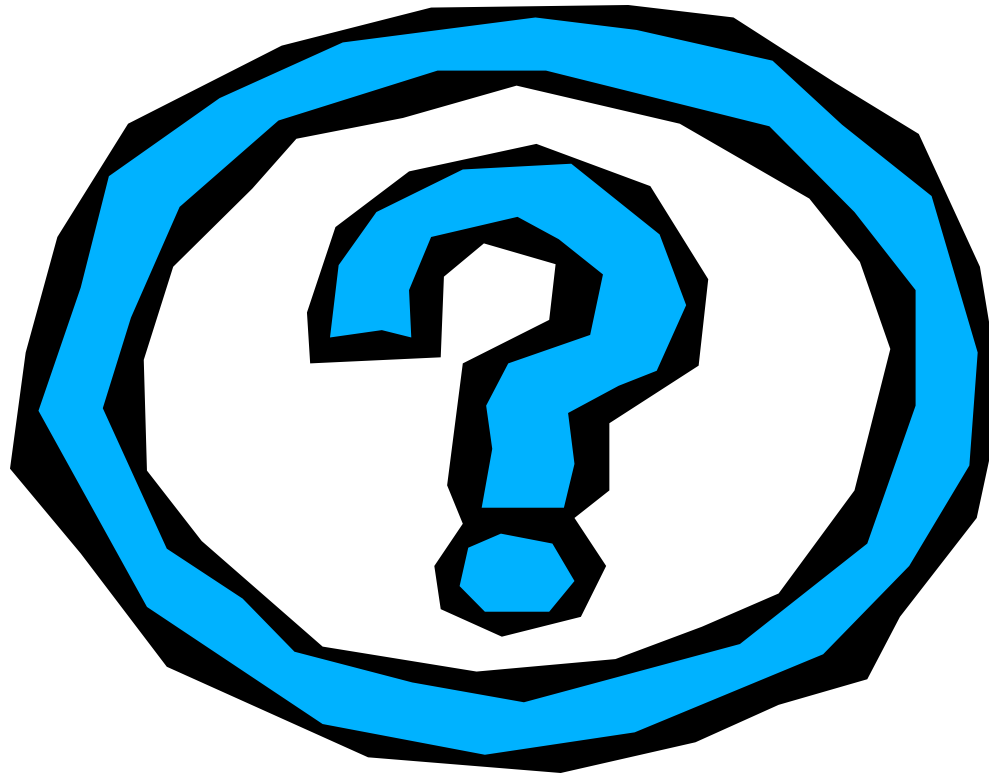
- Run real time virus protection
- Use a software firewall
- Use a spyware protection and detection program
- Disable operating system and software services not required for proper functioning

Data Backup and Recovery

- Use the "I Drive" when possible
- Backup files containing valuable information on a regular basis
- Maintain back-ups in a secure environment removed from the physical location of the computing device
- Verify ability to successfully recover backed-up files

Workstation Security

There is a lot we can do and the items reviewed are a very good start!



QUESTIONS?