Staff Security Briefing: Keeping Data Safe from Outside Threats

- 93H, Massachusetts Personal Identifiable Information Law(PII)
    - MA Consumer Protection law, enforced as of Spring 2010
    - Significant fines levied for data breaches of a name plus any of the following: SS number, financial account number, state ID card number, credit or debit card number.
- If a virus, trojan or other Malware is found on a PC, UMass is required by law to remove the hard-drive and begin a forensic analysis. If PII is discovered on the PC, all information, browsing history, etc, will be gone through thoroughly by the Chief Security Officer's team and reported to the UMass legal team. If a breach of PII is confirmed, by law the people whose identities were exposed must be notified and a fine will be levied for every record compromised. Either directly or indirectly, it is likely the press will be notified as well.
- The University may also begin an internal forensics analysis for breaches of information deemed "confidential" such as Student ID, Employee ID; anything deemed unacceptable for release to the public.

How to keep data safe:

- Keep no copies of PII or confidential information on the desktop or hard-drive.
- Keep *only* the PII which is currently required for job duties on the network shares, delete all other instances.
- Restart A&FS workstations daily; these restarts keep the machine patched and secure.
- Never download software onto an A&FS workstation.
- If a virus alert pops-up, immediately check with AFS before doing anything with the PC.
- Be wary of e-mail attachments, even from people you know. Use the network fileshare or the U: drive instead.
- Use a personal e-mail account for personal e-mail. Only use UMass account for professional use.
    - Ignore e-mail chain letters, be wary of FWDs containing media.
- Internet surfing, even mainstream websites, exposes the department to risk.
- Keep laptops up to date; use the OIT PC security checklist for home PCs if accessing any UMass services like Umail, OWA, WebDAV, Spire, etc..
  http://www.oit.umass.edu/security/protect/security_checklist.pdf
- Never share or write down your password. Keep passwords long and complex.
- Educate yourself about evolving security risks, discuss with co-workers and supervisors.
    - OIT security page -- http://www.oit.umass.edu/security
    - Travis' weblog -- http://blogs.umass.edu/tcroy/

Please contact Travis Roy with any questions or concerns.

tcroy@admin.umass.edu

v.1:4/28/10:TR