

Inappropriate Use of UVA IT Resources

Kevin Savoy, CPA, CISA, CISSP

Assistant Director of Audits – Information Technology





Agenda

- Current Status
- Law
- Policy
- Technical Aspects
- Procedures



Pornography Investigations

- Commonwealth law and UVA Policy prohibit state employees viewing and downloading of sexually explicit material via state resources.
- The Audit Department does not go out of its way to look for this activity. We act when it is reported to us.
- Must have permission from the President or Vice President of the area to review someone's computer activities.



Morality Police?

- I and my staff are not here to enforce morality.
- What employees do at home (unless criminal) that does not effect UVA is none of my business.



Past 14 months

- Ten investigations of staff / faculty.
- Seven (7) employees have left the institution.
- Egregious cases where employees were downloading thousands of pictures/movies.
- Some using peer-to-peer file sharing with users around the world.
- Some using “pagesucker” software to download whole websites.



What are the risks?

- Potential for Hostile Workplace lawsuits.
- Drain on IT resources (bandwidth, drive space).
- Pornography is infamous as a means to entice users to sites that are ripe with security risks such as viruses, Trojan horse backdoor software etc.
- Criminal activity such as child pornography.



It's a problem....

- SexTracker, a porn industry consultancy states that about 70% of all Web traffic to Internet pornography sites occurs between 9 a.m. and 5 p.m.
- The number of porn sites has vaulted eighteen fold, to 1.3 million, since 1998, says the National Research Council.



CODE OF VIRGINIA 2.2-2827.

Restrictions on state employee access to information infrastructure.

- Except to the extent required in conjunction with a bona fide, agency-approved research project or other agency-approved undertaking,
- **no agency employee shall utilize agency-owned or agency-leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content.**
- Agency approvals shall be given in writing by agency heads, and any such approvals shall be available to the public under the provisions of the Virginia Freedom of Information Act (§ [2.2-3700](#)).



Definition of sexually explicit

- We adhere to the law's definition of sexually explicit. (2.2-2827 and 18.2-390)
- This definition can be found at:
<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-390>



UVA Policy

- Mirrors the Commonwealth's Code of Virginia:

<http://www.itc.virginia.edu/policy/moreobscene.htm>
|



Degrees of Pornography

- Audit Department realizes that evidence of sexually explicit material can be left behind from accidental hit of a sexually explicit web site or received unsolicited via e-mail.
- We factor that into our investigations.



Technical Issues – Peer to Peer File Sharing (P2P)

- University environment is a sharing environment.
- P2P allows users to download parts of files from one another.
- Your computer may have 10 percent of a file the rest of the world is looking for. Thus you become a server for those users.



P2P continued

- It works great and was designed so everyone would not have to hit just one site to download a movie or whatever and thus overwhelm it.
- Two individuals were using it to collect and distribute adult pornography from UVA.
- It can be made into an automated process where you type the fetish that you are interested in and you begin to download and trade files with other Internet users.



P2P risks

- Potential is there to download and trade movies and pictures that you are unaware of.
- In essence, UVA or any business could become a server for child pornography if not careful.



Page Sucker and Vampire

- Examples of software that allow one to download the majority of the contents of a web site so that it is stored and viewed off line.
- One individual found to be doing this.
- The user assumption is that they will not be caught through Internet logs.



Generic log ins

- Many computers have generic logins so that it becomes hard to track offending parties.
- However, wherever possible it is best to institute individualized logins for accountability. (No one likes to be blamed en masse for another user's indiscretions).




Procedures

- Allegations of abuse should be made to Internal Audit or UVA Police (if it appears criminal).
- IT Audit and UVA Police are working closely together when criminal activities may be present.
- **DO NOT ATTEMPT** to investigate on your own as this may step on evidence and in a worst case scenario make it invalid for HR and/or criminal court proceedings.



LSP's role

- A few cases were brought to our attention when an LSP went to his manager to state that a user's system had sexually explicit material on it.
- In those case's the employee complained that his system was slow. (That will happen when you store 1000's of porn movies and pictures on your system!!)



LSP's role

- According to the UVA General Counsel's office, employees of the University generally are not at risk of personal liability for reporting potential legal and policy violations, if following set policy in good faith.



One last warning to anyone..

- The Internet **is not** anonymous.
- Trails of where you have been are all over the place.
 - Your own computer
 - Web site computer
 - Search engine computer
 - Internet Service Provider computer
 - Firewall server
 - E-mail server
 - Even router syslogs if implemented



Our Approach

- We have a checklist we have devised for these investigations
- DOS search for key words such as sex, porn, girl, boy, etc...
- Turn on Windows search to include hidden files – review Internet Cache and history
- If criminal activity is suspected make a forensic copy of the hard drive first!!
- We have utilities to restore deleted files such as deleted JPEGs
- We have utilities to change password to get into Window system
- We have utilities to review Apple Internet Cache
- DOCUMENT, DOCUMENT, DOCUMENT
- Create report



Questions??

- I can be reached at savoy@virginia.edu