Protecting your UCF computer

If you don't take proper precautions, hackers can break into your computer and steal sensitive information.

Hackers could wipe out information such as your class rosters, grades, projects, lectures, etc. This brochure lists ways you can secure your computer. You're responsible, under UCF Policies, for ensuring that your UCF computers and work areas are secure.

Password Security

- If it's in any dictionary or someone's name – it's a bad password: don't use it!
- Use a mnemonic, such as the first letter of a song verse or a phrase, while adding in numbers, symbols ($,%,*), and UPPER/lower case letters.
- Select a password that is a minimum of 6 characters.
- Change your password often! UCF standard is 60 days.
- Never write down a password and never share accounts.
- Do not give your password to anyone, not even the Helpdesk!
- Never use your UCF PID or password for non-UCF systems.
- Avoid the "save my password / remember my password" option on web sites.

Physical Security

Physically protect sensitive information and computing resources from criminals by following these simple tips:

- Always shut down or log off of any system when not in use.
- Protect your computer from power surges with surge protectors.
- Use password-protected screensavers.
- Make sure no one is looking over your shoulder when you enter your password.
- Lock your doors when you leave your office.
- Know who has access to your work area and computer.
- Properly dispose of (shred, etc.) all documents that contain sensitive information when they are no longer needed
- Never leave sensitive information (employee or student information, passwords, etc.) in plain view.
- Store backup copies of important files in a safe location.
- Store confidential or sensitive paper documents, data, and media in a safe location, such as a locked file cabinet or drawer.

UCF IT&R/Computer Acceptable Use Policy (AUP)
Responsibilities of Faculty and Staff:

UCF Information Technology Resources (IT&R) shall not be used to…

- impersonate another individual or misrepresent authorization to act on behalf of other individuals or the university.
- make unauthorized or illegal use of the intellectual property of others.
- attempt to read or duplicate electronic information belonging to others, or to decrypt or translate encrypted information
- send telecommunications messages the content of which is defamatory, or which constitutes a breach of telecommunications security, or is in violation of Federal, State, or local laws or university rules or policies
- intentionally damage or disable computing or telecommunications equipment or software
- undermine the security or the integrity of computing systems or telecommunications networks and shall not attempt to gain unauthorized access to these resources.
- A user must report any misuse of computer resources or violations of this policy to their department head, to the Information Security Office, to the Vice Provost or to the Chief Technology Officer at Computer Services & Telecommunications.

Misuses of Computing Resources include:

- Illegal acts.
- Failure to comply with laws, policies, procedures, license agreements, and contracts.
- Abuse of computer resources.
- Use of UCF computer resources for personal financial gain
- Failure to protect a password / account from unauthorized use
- Permitting someone to use another's computer account, or using someone else's computer account
- Unauthorized duplication and distribution of commercial software and other copyrighted digital materials
- Attempting to circumvent, assisting someone else or requesting that someone else circumvent any security measure or administrative access controls
- Unauthorized duplication or distribution of copyrighted material such as audio, video, pictures or text using a peer-to-peer application or with any other means.

Complete rules may be found here:

http://pegasus.cc.ucf.edu/rule.html

Information Security at UCF

Cyberknight insists that you safeguard your information and identity, and UCF's information and systems. Watch the video at

http://video.cst.ucf.edu

UCF
Stands For Opportunity

University of Central Florida
Information Security Office
Computer Services & Telecommunications
www.infosec.ucf.edu
www.cst.ucf.edu

Published August, 2007

Access to Sensitive Information (Student, employee, financial, medical, etc.)

- Sensitive information includes SS#, EMPLID, passwords, credit or debit card numbers, driver's license numbers, biometric data, medical records, student's non-directory information (PID, NID, grades, email address, photographs, etc.) and other information protected by law or policy.
- Social security numbers are no longer permitted to uniquely identify faculty, staff or students. The (Employee ID) or PID is the designated University ID Number. Replace social security numbers with the EMPLID or PID in your databases and spreadsheets and delete any records that are no longer needed containing social security numbers.
- Do not copy or download sensitive data from the University's administrative systems to your PC, Web server, PDA, Laptop, or any other portable device.
- Know the protection requirements for each type of data that you come into contact with. For more information consult with the information's custodian (e.g., Registrar, Human Resources, etc.)
- Some student directory information may be flagged at the request of the student as confidential and must not be disclosed. You may find more information at http://registrar.ucf.edu
- Avoid sharing information with unauthorized or untrained staff.
- Avoid non-work related disclosure of sensitive or confidential information. This includes student and employee information.
- Never store sensitive or confidential information on your office computer, laptop, or portable media. Instead, store it on a secured network drive. However, if you must store sensitive or confidential information on your computer for official business purposes, encrypt it. More information may be found at http://www.infosec.ucf.edu
- Never send sensitive or confidential information by e-mail or instant messenger. These methods of transfer can be intercepted and are not secure.
- Always secure sensitive documents. Never leave them in the open (i.e. on desks, etc.).
- Properly dispose of any sensitive documents or media that are no longer needed or being used. (e.g., shred papers, CD's, floppies)
- If there is sensitive information on your computer and you suspect the computer may be compromised do not make any changes to the computer or information. Contact your IT manager immediately!

Email Tips

- If you receive an email from a stranger, an in some cases from someone you know, never open email attachments or click on links embedded in the message without verification.
- Never respond to spam (unsolicited email) or click "remove me from mailing list" links—often that adds you to a list for more spam.
- Never respond to email solicitations requesting 'verification' or requesting personal information: this is likely a fraud or an identity theft scheme. This is phishing!

Spies Among Us?

When you install certain programs (such as filesharing-programs or shareware software) on your computer, you may unknowingly be installing spyware or adware programs as well. Spyware is a program that gathers information about you and what you do on your computer without your knowledge, sending the information to different sources. Along with raising many privacy concerns, spyware can also be a big nuisance to your computer, severely slowing it down and possibly causing frequent crashes. Adware may also be installed on your computer, causing multiple pop-up advertisements.

Patches and Updates

- Keeping your computer up-to-date with the latest patches is one of the best defenses against hackers and the spread of viruses and worms.
- Contact your network manager to find out if all of the software running on your UCF computer is up-to-date with the latest patches. To insure compatibility and security, contact your IT manager before installing or downloading any software.

Viruses and Suspicious Activities

- If you suspect your UCF computer has a virus notify your IT manager immediately.
- Never turn off your anti-virus program.
- Scan removable media (e.g., Floppies, CDs) for viruses before using them.
- Notify your IT manager if you notice suspicious activity such as the inability to login to your computer, constant computer crashes, abnormally slow programs, new files you did not create, deleted or missing files, or unauthorized persons in your work area.
- If you notice suspicious computer related activity **do not** turn off the computer or disconnect it from the network or make any changes before consulting with your network manager.
  - Forensic analysis may be necessary to determine the nature of the incident and what information may have been compromised.

Appropriate use and privacy

- The University of Central Florida provides computing resources for the purpose of accomplishing tasks related to the UCF mission.
- Use of UCF computing resources must be limited to justifiable computing support for academic and administrative purposes
- Use of UCF computing resources is subject to review and disclosure in accordance with the Florida Public Information.

File Sharing and Copyright

- File-sharing itself is not illegal; it's the files that are traded that cause problems. When you trade copyright protected material, you are breaking the law.
- University security incident response staff regularly investigates reports from copyright owners of file sharing and copyright violations. As a university we understand the philosophy of open communication and sharing of ideas and articles. However, we do not support sharing of ideas or articles that belong to private individuals or organizations.
- Since current peer-to-peer applications are predominantly used for trading copyrighted material, such applications are not permitted anywhere on the UCF network.
- For more information, please check the UCF Golden Rule and IT&R Rules, and the information security website:
  http://www.goldenrule.sdes.ucf.edu
  http://pegasus.cc.ucf.edu/rule.html
  http://www.infosec.ucf.edu

Protecting Your Identity

- Before purchasing resources on the internet or providing any personal information (bank account number, credit card number, etc.), always make sure that the Webpage is secure. Look for "https" in the web address (Notice the "s"). This shows the website is encrypted.
- Email is not appropriate for sending sensitive or confidential information, as most email providers do not provide encryption.
- Never collect credit card or bank account information via email. This violates UCF policy on appropriate methods for accepting credit card information. Look for cardholder information security procedures at http://policies.ucf.edu/