Antimalware Software

Malicious software, or malware, is written with malicious intent designed to infiltrate or damage a computer system without the owner's consent.

Most malware is designed to gather information, such as internet history or keystrokes in an attempt to gain passwords, and send the information to a third party over the Internet.

All computing devices capable of running antimalware software should have an antimalware solution installed and kept up-to-date. Recommendations are:

- MS Security Essentials or Windows Defender
- Adaware
- Symantec or McAfee versions that also provide malware protection

Watch out for Spyware

When you install certain programs (such as file-sharing 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.

Email Tips

- If you receive an email from a stranger, and in some cases even from someone you know, never open email attachments or click on links embedded in the message without verifying with the sender via phone or in person.
- Never respond to spam (unsolicited email) or click "unsubscribe" 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!

REPORTING AN INFORMATION SECURITY INCIDENT

To report an information security incident, such as unauthorized access to a university system or data, unauthorized usage of someone's account, or the accidental distribution of restricted data, please contact the Security Incident Response Team by using one of the following ways:

- Submit a ticket using Service Now at **https://ucf.service-now.com** or call the Service Desk at **407-823-5117**
- Email the Security Incident Response Team at **sirt@ucf.edu**

Protecting Your Identity

- Before purchasing resources on the internet or providing any account information, always verify the site and make sure that it is secure. Look for "https" in the web address (note 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 send credit card, bank account information, or your Social Security Number via email or instant messaging.

Common Sense and the Internet

The Internet is a vast resource of knowledge, but it is also filled with dangers. Some dangers can be avoided by using common sense.

Social media sites can be fun ways to express yourself. However, setting up profiles that contain personal information such as home address, phone number, or birthday should be avoided. Additionally, you should avoid posting information or images which could be damaging to UCF or to you.

Don't become a victim - keep your personal information off the Internet. Information such as your full name, home address, phone number, Social Security Number, and account information such as bank and credit card numbers should not be shared online.

Sharing too much increases the odds that your system or personal information could be compromised.

UCF

Information Security for Students

Use of UCF computing systems in any way contrary to applicable Federal or State statutes, or the policies of University of Central Florida is prohibited and will make you subject to University disciplinary action, including possible immediate suspension, and may also subject you to criminal penalties and/or prosecution.

INFORMATION SECURITY OFFICE
UNIVERSITY OF CENTRAL FLORIDA
WWW.INFOSEC.UCF.EDU
INFOSEC@UCF.EDU

Introduction

As an institution of higher learning, the University of Central Florida encourages, supports, protects, and embraces freedom of expression to pursue scholarly inquiry and to share information with the global academic community.

To maintain a secure and reliable network, UCF Information Technology strives to inform all UCF employees and students of the policies which govern the use of UCF computing services and networks.

This brochure is designed with students in mind. In it you will find information on where to find policies and tips on how to secure your computer and pitfalls to avoid.

Computer Policy & the Law

By using UCF networks, computing services, and other computer resources, you accept and agree to all policies governing their use. The policies for Appropriate Computer Use can be found at

www.policies.ucf.edu

Each user is responsible to read, understand and remember computing policy. Users can seek clarification from Information Security Office at **infosec@ucf.edu**

Computer Use & the Law

Information technology is not only governed by the University itself, but also by state and federal laws and regulations. Therefore, the following may apply to the data stored and transmitted on the network:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Florida Statutes
- Florida Computer Crimes Act
- The Digital Millennium Copyright Act
- General Data Protection Regulation (GDPR)

Copyright Infringement

A copyright infringement occurs when you download, store, use, copy, or share, something created by someone else without the permission from the person or entity that created it. Violating copyright is against UCF policy and Federal law.

- University security incident response staff regularly investigate 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 UCF Policies & Procedures, the UCF Golden Rule, and the Information Security Office website:

🌐 www.policies.ucf.edu
🌐 www.goldenrule.sdes.ucf.edu
🌐 www.infosec.ucf.edu

Computer Security

Computer security is everyone's responsibility. The following information will assist you in securing your personal information.

PASSWORDS

- 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 8 characters.
- Change your password often! UCF standard is 60 days.
- Never write down a password.
- Do not give your password to anyone, not even the Service Desk!
- Never use your UCF network ID (NID) or password for non-UCF systems.
- Avoid the "save my password / remember my password" option on web sites.

Protect Your PC

FIREWALLS

If your computer is connected to the internet you should have an active and correctly configured firewall. Check with your operating system vendor for more information.

PHYSICAL SECURITY

Physically protect your computing resources from criminals by following these simple tips:

- Use password-protected screensavers.
- Make sure no one is looking over your shoulder when you enter your password.
- Store backup copies of important files in a safe location.

PATCHES AND UPDATES

Downloading and installing the latest security patches and updates for your operating system and programs, and enabling the automatic update feature, significantly reduces the chance of your system being compromised.

Antivirus Software

Computer viruses attach to legitimate programs or executable files. They vary in their specific task, but they usually work the same. When an infected file is executed, the virus is also executed. The virus can then follow its programming and complete its task.

Viruses are grouped into several categories: plain viruses, e-mail viruses, worms, and Trojans.

Having up-to-date antivirus software on your computer is a necessity to protect against such malicious software. There are many antivirus solutions available, including Microsoft Security Essentials, Symantec, and McAfee.