Security Essentials

Don't be the weakest link, practice the Security Basics

- *Never store Restricted information on removable media such as thumb disks, memory sticks, or cd's; they're too easy to lose track of*
- *Never put Restricted information in email or in an instant message*
- *Encrypt Restricted information that you must store on your laptop or PDA*
- *Never leave laptops or personal digital assistants (PDAs) unattended and unlocked, not even for a minute; they're highly desirable, and very easy to steal*
- *Use a strong password (min 8 chars and contains at least 1 letter, 1 number, 1 capital, 1 lower case, and 1 special character) on your computer so it cannot be easily guessed*
- *Ensure you have set an inactivity timeout on your computer so it automatically locks requiring a password to unlock*
- *Your computer activity and patient record accesses are tracked by HSC Information Sys-tems; we know where you've been*
- *Always wear your Gator 1 ID badge at all times. It helps us determine when someone else is in a place they should not be*
- *If you're not sure about appropriate handling of Restricted Information, ASK for HELP!*

University of Florida Portable Computer Support Resources

For help with network registration and confi gu-ration, Windows security patching, anti-virus software installation/updating, Spyware removal, data backup, or general support, visit:

College of Pharmacy:
HPNP Building, Rm. 4303;
support@cop.ufl .edu

College of Public Health and Health Professions:
HPNP Building, Rm. 4130;
support@phhp.ufl .edu; 273.6200

College of Veterinary Medicine:
Rm. V2-102; help@mail.vetmed.ufl .edu;
392.4700, Ext 4357

College of Dentistry, Nursing, Medicine, and Other HSC Units:
Communicore, Rm. CG-58;
itcsupport@vpha.health.ufl .edu

UFHSC SPICE

Security Program for the Information and Computing Environment

Information Security Reference Guide for Personally Managed Computers and PDAs

UFHSC SPICE The Focus is on you
Security Program for the Information and Computing Environment

http://security.health.ufl .edu

UF UNIVERSITY of FLORIDA
Information Technology

SPICE Information

So You've put off learning about Information Security until now. Unfortunately, you can't put it off any longer. As a faculty or staff member at the UF HSC, you have responsibilities to protect confi dential information. The stakes are high and serious consequences apply to the misuse of Information.

The UF HSC defi nes Restricted Information as Data whose loss, corruption, or unauthorized disclosure would seriously and adversely impact the academic, business or research functions of UF HSC. The following types of information are protected by Federal and State laws on privacy, and are classifi ed by the UF HSC as Restricted. Whenever you have this informa-tion in your custody, you must protect it from accidental disclosure and you must not share it without authorization.

- *Protected Health Information (PHI) - Health information combined with name, or med record #, or address, or key dates, or family members, or any other information that would link a person to their health condition*
- *Personal Identifi cation Information (PII) -Names combined with SSN, ID Numbers, or any information that could be used to commit identity fraud*
- *Student Records - Name or UF ID combined with grades, demographics, or any information shared by faculty and staff about students*

Securing Your Portable Computer

The SPICE Approach

Anti-virus Protection

Anti-virus protection is needed to fend off viruses or worms that can cause your computer and software to fail and cause you to lose data. Your computer may have come with anti-virus software pre-loaded, but it may not stay current if you don't pay a subscription fee. Anti-virus software that is not current is useless. UF has purchased McAfee Anti-Virus software for all faculty, staff and enrolled students to use. Here's what you can do to protect from viruses at no additional cost to you:

- *Download a copy of McAfee Anti-Virus software from http://www.software.ufl .edu/mcafee*
- *Follow all download and installation instructions carefully, even downloading VPN software which is safe*
- *Enable AutoUpdate and schedule it for daily updates*
- *Enable Scan All Fixed Disks and schedule a scan at least weekly when you know the computer will be on*

Note: If you are having trouble getting McAfee Anti-Virus software to work, and if you have another Anti-Virus product installed on your laptop, the problem could be related to compatibility issues between the two products. Use the Add or Remove Programs feature in your Control Panel to remove the product.

System Patches (Windows pcs)

System patches are operating system software updates intended to fi x bugs and weaknesses in the Windows operating system that have recently been discovered. It is easy to have them automatically installed on your computer so you don't have to re-member to do it yourself, and it is so important to the health of your computer.

- *Go to this safe link to sign up: http://www.microsoft.com/microsoftupdates/*
- *Follow the download instructions carefully*
- *Set the updates to automatically check and install daily*

Email Attachments, HTML pages, URLs

Opening attachments, displaying HTML pages and clicking on URLs sent to you in an email are the most common ways to contract viruses and worms.

- *Delete email from unknown senders*
- *Call and verify if you receive an unexpected attach-ment, HTML page or URL from someone you know, before you open it*
- *Legitimate Email can always be sent again*
- *Regardless of who sends it, do not open fi les that end in .exe, .bat, .vbs, .pif, or .com*
- *If it sounds too good to be true, it is*

Spyware and Adware

Spyware is software deposited on your computer that seeks to gather private information about you. There is a free and safe software utility called Spybot Search&Destroy that helps control spyware.

- *Download Spybot S&D on your computer from http://www.safer-networking.org/en/download/*
- *Use the advanced features of Spybot to enable Au-tomatic Updates and Schedule Scans at least weekly to keep your include fi les and Spybot version up to date*

Adware is software deposited on your computer that gathers information about what web sites you visit and your buying habits, and sends it to a company for marketing uses. It subsequently causes pop-up ads on your computer screen, which are annoying and somewhat invasive. There is a free and safe software utility called Ad-Aware SE Personal that helps control adware.

- *Download Ad-Aware SE Personal on your computer from http://www.lavasoft.de/software/adaware/*
- *Unfortunately updates can not be automated with the free version of Ad-Aware*
- *Check for and download defi nition fi les and program updates at least weekly and run an Adaware system scan thereafter*

Social Engineering

Social Engineering is best described as a con man who is trying to dupe you into doing something you wouldn't ordinarily do. You might get offi cial look-ing email asking you for your password or fi nancial account number for 'security' purposes. You might get an enticing email indicating you have won an extravagant vacation, telling you to click a URL, and enter personal information to collect your prize. You might be downloading software, and be prompted to accept the terms of a lengthy license agreement with language permitting the company to install spyware or adware on your computer with the software you want.

- *Be wary of unsolicited offers and notifi cations asking for personal information. Never give up personal infor-mation on your computer due to an unsolicited email or notifi cation*
- *If you think an unsolicited notifi cation asking for personal information is legitimate, call the institution rather than conducting the exchange on your com-puter*
- *Be wary of license agreements that are discouraging to read, but contain language permitting the installa-tion of spyware or adware programs on your computer. Of course it won't be called spyware or adware in the license agreement*
- *If it sounds too good to be true, it is*

Data Backups

Backup your important fi les and folders regularly and consistently to protected fi le space that the UF pro-vides on network servers. We want you to be produc-tive at the University of Florida. Don't risk losing your data. Accidents WILL happen. Your hardware WILL eventually fail.

Encryption

Storing confi dential information on laptops, PDAs, or removable media is very dangerous and should only be done when absolutely necesary. If you must do so, make sure you have an encryption solution. The following are viable encryption software, but you should read the documentation very carefully to install and use them properly:

- *Windows PCs: PGP WDE Professional or XP ver-sion of EFS (Note: donâ€™t use EFS for Windows 2000)*
- *Macs: FileVault*
- *Removable media accessible by Windows and Linux: TrueCrypt*
- *Removable media accessible by Macs: PGP Vir-tual Disk or PGP SDA*

Internet

Safe web sites and trustworthy internet users are not apparent. Exercise these internet use cautions:

- *Be judicious about picking legitimate web sites to visit; stick to those that are widely known businesses or institutions, and those that you have visited be-fore without security issues*
- *Make sure the controls listed in this reference guide are in place on your computer*
- *Never offer up private information in email, instant messaging or on a web site that has been unexpect-edly solicited from you*
- *Email and instant messaging are no place for Restricted Information in any event*
- *Remember, if it sounds too good to be true, it is*