



UNIVERSITY OF
SOUTHERN MAINE
Division of Information
and Technology

10 STEPS TO DATA AND NETWORK SECURITY

Much of the information stored electronically at the University is sensitive financial, personal, medical and otherwise private information. Unauthorized dissemination or access to data and the University network is unethical and, possibly, illegal. Personal liability can be incurred whether either is compromised intentionally or inadvertently.

There are several statutory privacy requirements we must follow (HIPPA, GBL, FERPA, etc.) to prevent the unauthorized dissemination of this information. While following the suggestions below will not guarantee full compliance, they will help by providing affirmative evidence of our compliance efforts. The responsibility rests with the design and administration of the University Network and relies upon you to adhere to best security practices.

The purpose of this document is not to identify what is or is not sensitive. Rather, there are a number of practices we have fallen into that are an open invitation to unauthorized access. There are 10 simple changes in work behavior that would go a long way in limiting our vulnerability to unauthorized access and dissemination of confidential data.

1. Use a strong password and keep it a secret

The key to accessing the network is your password. In order to reduce the chance of a computer or another person guessing your password, you should choose a strong one. A strong password is a combination of letters, numbers, and symbols that is NOT a word or common phrase. Your password should not be a word from the dictionary or one that someone with a little personal knowledge of you might guess (i.e. your child's name or your phone number). As well, the password you use to access University resources should be unique from those you use to access resources outside the University, and, most importantly, you should **never** share your password with anyone or write it down anywhere.

University support technicians, including those at the USM HelpDesk, will NEVER ask you what your password is. One of the most common password-stealing tricks employed by hackers and information thieves is to call on the phone and impersonate a company's help desk staff or network administrator. Don't fall for it. If you receive a call or email requesting your password, you should refuse to provide it and immediately report the incident to the HelpDesk (780-4029 or helpdesk@usm.maine.edu).

In situations where you initiated a call to the USM HelpDesk, the technician assisting you may set a temporary password on your account for their use. They will only do that with your approval, and only if other troubleshooting measures have failed and using your credentials will allow the technician to test the problem firsthand. After the troubleshooting is complete, you will be required to change your password immediately.

2. Do not let another person use your user account

Your user account represents all the computing resources that you personally have been authorized to access. By letting someone else use your user account you are letting them access resources for which they do not have approval. Anything that they may do will, ultimately, be your responsibility.

3. Use network drives for sensitive or important files

All files that contain sensitive information, or that are critical to the University's work should be stored on a network drive – but only as long as they are needed. These are usually the drives with higher letters in the alphabet above “F:\”. Why use network drives?

Security: Anyone with physical access to a computer can, one way or another, get access to the files stored on the computer’s local drives - A:\ through E:\.

Data Protection: If a computer "crashes," then all data on the local drives might be lost. Files stored on the network drives are backed up on a nightly basis. In the event data is lost due to some disaster, there is a much greater chance that the data can be restored to a relatively recent state.

4. Lock your computer when away from your desk during the day

The world's strongest password won't matter at all if you walk away from your desk, even for a few minutes, and leave your computer on and unlocked. For computers running Windows 2000 and Windows XP Press Ctrl-Alt-Del key simultaneously and select *Lock Workstation*. When you return to your desk you will have to enter your Novell password to unlock the computer. For Mac workstations using OS X, you can password-protect your account under "System Preferences" to be activated every time the computer goes into Sleep mode.

While you are at your computer you should arrange your work area so that your screen cannot be viewed by casual visitors. This can alleviate a lot of inadvertent viewing of personal or confidential information.

5. Shutdown your computer when you leave for the day

When you leave the office each night, turn off your computer. A computer that is off cannot be infected or compromised by attacks from other computers.

6. Use encryption for viewing and exchanging sensitive data

You should always use encryption to view websites containing sensitive data. You can tell if a website is using encryption if the web address begins with "**https**".

If you have created a website that collects sensitive data you should be sure that the site forces users to use encryption when submitting data and that the data, once submitted, is being stored securely.

Remember, email is not encrypted and therefore should not be used to exchange sensitive data. If you have need to transfer sensitive data via email, the information should be sent in a password-protected zip file attachment. Tell the recipient the password in person or via the telephone, not via email. For a corollary caution see #8.

Finally, remember that when using wireless connections, they are not secure. Any data you may be accessing can be captured someone using similar technology. When accessing data and information that is confidential you should only use a connection that is hardwired to your machine.

7. Do not install unapproved software

Only the programs found in Start – USM Apps – Install have been approved for installation on University computers. If you feel you need to install a piece of software not found there, you must get the approval of DoIT staff first.

Do not install free software found on the Internet. These programs often present a great security risk. To avoid this be very wary, when surfing the Internet, of pages that offer anything for free by just “clicking here”. If unexpected pop up messages are displayed while surfing the Internet use the “X” in the upper right corner of the message to close it.

8. Think before opening email attachments

Be suspicious of emails with attachments that you were not expecting to receive even if they appear to be from someone you know. If it appears to be from someone you know, before you open it, contact them and confirm that they intended to send you the attachment. For a corollary caution see #6.

9. Schedule an antivirus scan of your computer

Most of us have a weekly staff meeting. At these times your computer is usually sitting idle in your office. That is a perfect time to schedule an antivirus scan of your computer to run. These can run while your computer is locked. If any viruses are detected, please report them to the HelpDesk.

10. Be careful using Internet Explorer

We feel it is best to only use Internet Explorer for those websites that require it (i.e. PeopleSoft) and use a different browser for all other web activity. The Internet Explorer web browser that comes with Microsoft Windows seems to have a new security flaw almost every month. While we apply patches for these flaws as quickly as possible, DoIT recommends the use of Mozilla’s Firefox, available via Start – USM Apps – Install – Firefox Web Browser. You need to get approval before installing any other browser.