Hello,

The Information Systems Planning and Support unit recently ran a password cracking program against our local OCP network accounts file and found that some passwords were successfully cracked within seconds, others took several hours—which means that we could tell these users exactly what their passwords were at that time. We have notified those users of the need to change their passwords, however, we feel it's important to inform all network users of the security work that's being performed and why.

The protection of University data relies on many factors but one of the most basic is account/password access. Protecting University information is important to all of us so we urge you to make all your passwords as complex as possible given the constraints of systems (some, such as PPS do not allow the use of punctuation, non-alphanumeric, or extended ASCII characters) and your ability to remember your passwords (a password's no good if it's so complex you have to write it down on a post-it note near your computer).

The security improvements we've implemented since January, including IP Security on workstations, firewalls on our servers, password testing (e.g., cracking), password-protected screensavers, etc., are NOT the result of any incident—they are improvements that have been long-planned and are now able to be implemented due to our move earlier this year to an Active Directory network and having the time and manpower required to research, test, and implement the changes.

We've appreciated your cooperation and feedback. We believe security should be implemented with an eye to maintaining a balance of system usability and limiting access. The most secure computer is one that has several layers of security including complex BIOS and workstation passwords, multi-factor authentication (e.g., BANNER's hard token and system logon), located in a locked room, and not connected to a network. This system, however, is not usable for our purposes.

Rationale

The object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about what you've chosen.

Why We Need Passwords

Security: Measures adopted to guarantee freedom or secrecy of action, communication, or the like.
Password: A secret word or phrase that one uses to gain admittance or access to information.
Like the key to your home’s front door, your password keeps out unwanted intruders. Would you leave your house keys lying around to be picked up by just anybody? And in this day and age, how many people hide their keys underneath the front door mat? So then, why are electronic passwords still scribbled on sticky notes on computer screens or stashed under keyboards or in the back of desk drawers?

**Why is security important?**

Someone who guesses or steals a password can conceivably access files, e-mail messages, funds, and personal information. This access may allow the hacker to change or destroy files or send e-mail threats in someone else’s name. And this chaos can extend beyond just one account. Once intruders gain access to a system, they can monitor other machines and systems on the same network and even monitor the remote systems to which the local users connect. Furthermore the hacker can install key logging software that records every keystroke made on that computer. All keystrokes including those when you're logging onto our network, entering your credit card information for an online purchase, and accessing your online banking information. An unwanted intruder might, by way of a stolen password, gain access to confidential University information relating to negotiations, project plans, communication strategies, performance appraisals, etc.

The use of individual accounts and complex passwords is not only important for restricting unauthorized people from accessing University systems, such security is also important to keep employees from accessing, altering, or destroying materials.

Although we hope that everyone enjoys positive, convivial relationships, such is not always the case. There are numerous corporate examples of employees who when angered, destroy historical correspondence, records, etc. If someone has your password, they can modify or delete your documents and send messages which appear, to all intents and purposes, to be from you.

**Simple passwords won't work after August 17**

ISPS will be implementing a network-based policy in August that will require increased password complexity on all OCP network accounts and will **not** allow a user to logon if his/her password does not meet the password complexity criteria listed below. Please note that the guidelines below are the same ones used for campus computing accounts so you should be able to match your campus account password to your local OCP account password, if you so desire.

Please remember that the more accounts on which you use the same password, the more important it is to keep that password only known to you! ISPS staff can quickly provide access to departmental e-mail and network and local data directories given the proper approvals.

**How do I change my password?**

9/23/2003
You can change your local OCP network password by performing the following actions (ISPS staff will be pleased to assist you if you experience difficulty or have questions):

**How to change your OCP network password**

1. Logon to local OCP network
2. Press CTL-ALT-DELETE keys on keyboard
3. Press the CHANGE PASSWORD... button on screen at the resulting prompt
4. Enter your current OLD PASSWORD->press TAB key
5. Enter your NEW PASSWORD->press TAB key
6. Enter your new password again at CONFIRM NEW PASSWORD prompt
7. Press the OK button on screen
8. Your password should now be changed

**Password complexity criteria**: Your password...

- must be seven (7) or eight (8) characters long
- must contain at least one uppercase (Capitalized) letter
- must contain at least one lowercase letter
- must contain at least one numeral (0 through 9)
- must contain at least one punctuation character
- **may not** contain any spaces
- **may not** contain any of the following characters: " & ; ' ` (double quote, ampersand, semicolon, single quote, and back quote)

Again please note that these criteria are the same as the University's computing account criteria. In actuality, you could make your OCP password much more complex and therefore much tougher to crack. Windows 2000 and Windows XP allow passwords up to 127 characters long. If the password is longer than 15 characters the weaker LanMan hash will not be stored and the password will be much more difficult to crack. The use of extended ASCII characters also greatly decreases the likelihood that your OCP password could be hacked ([http://mmdev.ag.vt.edu/security/YmcaOU%20HTMLs/Strong%20passwords.htm#_Extended_ASCII_characters_1](http://mmdev.ag.vt.edu/security/YmcaOU%20HTMLs/Strong%20passwords.htm#_Extended_ASCII_characters_1)). Please note that using extended ASCII characters limits your ability to access Outlook information via web access from Macintosh computers.

**What Not to Use**

- Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse’s or child’s name. Passwords should not be the name of a pet, a favorite rock group, city, town, common word, etc. since these may be easily guessed. In short, do not use names.
- Don't use other information easily obtained about
you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.

- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words. One online dictionary available is http://dictionary.reference.com/
- Don't use a password shorter than seven characters.

What to Use

- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Method to Choose Secure and Easy to Remember Passwords

- Choose a line or two from a song or poem, and use the first letter of each word. For example, "My daughter, Shelly, likes apples" becomes "Md,Sl,a." Whereupon you can add a number and you're done!

Keep your Password Confidential!

- Do not write a password on sticky notes, desk blotters, calendars, files, or store it online where it can be accessed by others.
- Do not share your password with anyone.
- Do not use your OCP network account for other non-University systems such as Amazon, your bank, Microsoft PassPort, PayPal, etc. as their security can't be assured. If they are hacked the hacker now has the password to your University systems.

Web Access

When entering password information via the web, please look for the gold lock which should be located in the lower right corner of Internet Explorer. This gold lock ensures any passwords and subsequent data you submit via that web page is sent via an encrypted (e.g., not plain text) channel. Our Outlook Web Access uses such encryption.

INFORMATION RE: CHANGING OTHER UNIVERSITY SYSTEM PASSWORDS

Other systems have different password criteria regarding how often the password must be changed, how often passwords can be recycled, complexity, how many levels of authentication are required (i.e. hard token), etc.

- University Computing Account (aka UCD LoginID) - includes campus modem pools, MyUCDavis portal, DaFIS Decision Support, and other services
- How do I change my unique password?  
  [https://computingaccounts.ucdavis.edu/cgi-bin/services/index.cgi](https://computingaccounts.ucdavis.edu/cgi-bin/services/index.cgi) (second option on left)
- How do I change my Kerberos password? [https://computingaccounts.ucdavis.edu/how.html#change](https://computingaccounts.ucdavis.edu/how.html#change)
- Computing Accounts Service ID Descriptions - [https://computingaccounts.ucdavis.edu/descriptions.html](https://computingaccounts.ucdavis.edu/descriptions.html)
- What access (services) does my University account have? [https://computingaccounts.ucdavis.edu/how.html#view](https://computingaccounts.ucdavis.edu/how.html#view)

- **BANNER**

- How do I change my Kerberos password? [https://computingaccounts.ucdavis.edu/how.html#change](https://computingaccounts.ucdavis.edu/how.html#change) (please note that this changes the password for your UCD Computing Account and associated services as well)

- **DaFIS**

  - DaFIS doesn't use Kerberos, though you can set up your DaFIS password to be the same as your Kerberos password. Changing your Kerberos password thereafter doesn't change your DaFIS password; there is a separate process for that.

- **PAYROLL/PERSONNEL SYSTEM (PPS)**

  - PPS How do I change my password? - [http://sysdev.ucdavis.edu/ppsdoc/passfaq.htm#c](http://sysdev.ucdavis.edu/ppsdoc/passfaq.htm#c)

- **Data Editing System for Instructional Information (DESII)**

  - How to contact the DESII Team - [http://www.iais.ucdavis.edu/desii/contact.html](http://www.iais.ucdavis.edu/desii/contact.html)

If you have any questions, please let me or any of the ISPS staff ([ocptech@ucdavis.edu](mailto:ocptech@ucdavis.edu)) know.

~Sharie

===========================================================================
Sharie Sprague - Manager, Information Systems Planning & Support
Offices of the Chancellor & Provost/Mrak Hall, 5th Floor
University of California, One Shields Avenue, Davis, CA 95616
Voice: 530-752-9928/FAX 530-752-3832/E-Mail: sasprague@ucdavis.edu
===========================================================================

9/23/2003