

➤ **How to create a “Strong” Password:**
Addressing a “weak link” in the protection of electronic research data
(A system is only as strong as its weakest link.) ➤

Why do I need to have a “strong” password?

Researchers are responsible for developing security procedures for ensuring the confidentiality and integrity of both electronic and hard copy research data. The protocol and consent document indicate that collected data will be protected and how that will be accomplished. While paper documents may be adequately protected by storing them in locked file cabinets in secured areas, the security of electronic data requires special consideration.

Computers are among the most valuable tools used in conducting our research. We all recognize their value – but what is often inadequately acknowledged and addressed is their vulnerability to unauthorized access.

Even with the finest electronic data security systems in place, the strength of the system rests with its weakest link, which, in many instances, involves the use of poor passwords by individual users. A weak password may give a hacker access not just to one computer but to the entire network to which the computer is connected. “Weak” passwords that once took months to crack can now be determined in minutes. For instance, it takes less than 3 minutes for password-cracker software to check all possible letter combinations for a six-letter password that uses all upper case or all lower case letters.



This issue of HRPP Topics focuses on the need for research staff to use “strong” passwords and how to create them.

Use of “strong” passwords is a simple, inexpensive, and effective line of defense against malicious intruders. Generally, “strong” passwords should be used in conjunction with other electronic data security measures to guard against data access, tampering and/or destruction. “Strong” passwords alone, however, provide invaluable protection at the individual level.

At a minimum, research data stored on desktop computer, laptop, PDA, storage disks, or USB jump/flash drives, should be protected with a “strong” password. To provide additional security, consider using an equally “strong” password to protect individual files.

What is Password “cracking”?

Password “cracking” is the process of figuring out a password to gain access to a system or an account to which you don’t have authorization. Password cracking software may use guessing, dictionary attacks, or automation that tries every possible combination of characters. Given adequate time, the automated method can crack any password. “Attack dictionaries” permit every word in any language dictionary to be tried in minutes. Names, common misspellings, words with numbers, and other commonly used passwords are also tested. Remember: computers don’t get tired – they can work 24-7 trying to figure out your password.

What is the difference between “hacking” and “cracking”?

Machines are “hacked.” Passwords are “cracked.”

How can I create a “Strong” Password?

Use **AT LEAST 3** of four kinds of characters:

- o Upper Case letters: **A-Z**
- o Lower Case letters: **a-z**
- o Numbers: **0-9**
- o “Special Characters”: **!@#^&*()_+=|~`{[]};" '<, > ? /**

Note: Passwords *MAY NOT* include blank spaces or control characters such as a return tab. Also, some systems will not accept certain special characters. You may need to check with your computer/network administrator if you have problems using certain characters.

Use a **minimum of 8** characters:

The fewer types of characters you use, the longer your password should be.

Note:

For Windows Users: Windows 2000/XP passwords can be up to 127 characters long. However, Windows 95 and Windows 98 only support passwords of up to 14 characters.

For Non-Windows Users: Non-windows systems may have different maximum characters. Consult your computer/network administrator for the maximum number permitted for your system.

Do Not Use...

- o Any portion of your full name or username
- o Any names that link back to you such as: your own name or names of your family, friends, pets, children, etc.
- o Birthdays or other personal information such as addresses or phone numbers
- o Words that can be found in any dictionary (English or foreign language)
- o Sequences of repeating characters or adjacent letters on your keyboard such as: &&&&&, gggggg, 55555, defghij, qwerty
- o Bank pin numbers, credit card numbers, or other ID numbers
- o Any of the above spelled backwards
- o Any of the above preceded or followed by a digit (e.g., tabby3)

Can you give me ideas for creating “strong” passwords that I can remember?

Choose two or three words, capitalize the first and/or last letter of the words, and join them together with a punctuation character or number:

Examples: **Banana?peeL** OR **Dairy8Queen8Sundae**

For even stronger passwords, try thinking of “phrases”:

Think of a phrase that is meaningful to you so you can remember it. Then convert each word of the phrase to a corresponding number, character, or upper or lower case letter.

Example 1: “I love to look for lobsters in Maine” could become the password: **I!2%4LIM**

Example 2: “There are 50 states in the US” could become the password: **ta50sitUS**

What should I do if my password that accesses research data is stolen?

If you believe that there has been, or is the potential for, a breach of security/confidentiality with regard to research data, **notify the Principal Investigator immediately!**

How do I change my password?

Changing your UBITName password:

The following link provides you with instructions: <https://ldap.buffalo.edu/cgi-bin/chpass.pl>

Changing other passwords that access study data:

Check with the Principal Investigator and/or your computer/network administrator regarding specific guidelines for your system.

What can I do to protect my password?

- o Don't tell anyone your password!
- o Do not tape your username and password on the computer screen!
- o Do not use the same password for multiple accounts.
- o Don't let anyone watch you type in your password.
- o Safeguard any passwords you have written down.
- o Change your password(s) often: this limits the amount of time someone has to guess your password and the amount of time the password can be used if it is “stolen.”
- o Never provide your password over email or based on an email request: Email messages that request your password or that direct you to go to a Web site to verify your password are called "phishing" emails. Responding to these emails and revealing your user names and passwords and/or other personal information could have serious consequences including identity theft. Reputable financial institution or business will never send you an email requesting that you provide personal account information online.
- o Do not type passwords on computers that you do not control such as those in Internet cafés, kiosk systems, conferences, and airport lounges. Do not use these computers to check any accounts that require a user name and password. Inexpensive “keystroke logging” devices can be installed in just a few minutes and allow malicious users to harvest all the information typed on that computer.

What are other password tips for protecting data files from unauthorized access?

- o Grant password permissions only to those who require access to the data in order to do their jobs.
- o Require password protection for all transportable data on laptops, PDAs, storage disks, or USB jump/flash drives, etc.
- o Password-protect copied or backup disks and keep them in secure storage areas.
- o Set your security system to “Require” passwords to be changed on a regular basis: e.g., every 6 months.
- o Deactivate password authorization to access data as soon as possible within 24-hours for staff who discontinue employment.

