

January 2008

Password Security

Your computer and data are only as safe as the password you use to access them. Passwords are the "keys" and ultimately the last layer of defense between your sensitive data and hackers and should be treated like the keys to your car or the access codes to your bank/credit cards. Passwords authenticate that you are who you claim to be. If someone authenticates as you, they are then authorized to do anything you could do on your computer or account.

Every year the number of computers and data illegally accessed because of weak passwords grows. For convenience sake, most users choose passwords that are easy to remember. Unfortunately, the easier the password is, the easier it is for a hacker to guess it. One of the first things a hacker will do against a system is run a program that will attempt to guess the correct password of the target machine. These programs contain entire dictionaries from several different languages. In addition to words found in dictionaries, these programs often contain names, words from popular culture such as movies, songs and novels, application default passwords, list of the most common passwords used (i.e. password1, password2) and common character sequences such as "123456" or "abcdef". This is why it is so important to use strong passwords, and not share them.

Consider the following when creating passwords:

1. **Longer is stronger.** Each character that you add to your password increases the protection that it provides many times over. Passwords should be 8 or more characters in length; 14 characters or longer is ideal. Many systems support the use of the space bar in passwords, so you can create a phrase made of many words (a "pass phrase"). A pass phrase is often easier to remember than a simple password, as well as longer and harder to guess.
2. **Use a combination of upper and lowercase letters, numbers, and symbols.** The greater variety of characters that you have in your password, the harder it is to guess. Other important specifics include:
 - **The fewer types of characters in your password, the longer it must be.** If you cannot create a password that contains symbols, you need to make it considerably longer to get the same degree of protection. An ideal password combines both length and different types of symbols.
 - **Use the entire keyboard,** not just the most common characters. Symbols typed by holding down the "Shift" key and typing a number are very common in passwords. Your password will be much stronger if you choose from all the symbols on the keyboard, including punctuation marks not on the upper row of the keyboard, and any symbols unique to your language.
3. **Use words and phrases that are easy for you to remember, but difficult for others to guess.** The easiest way to remember your passwords and pass phrases is to write them down. If you write them down they must be adequately protected in order to remain secure and effective.

Additional security measures to protect passwords:

- **Never share your password with anyone.** As the owner of the account you are responsible for all activity (legitimate or illegitimate) associated with that account.
- **Never save your password if prompted by your browser or any other programs.** By storing your passwords so you don't have to enter them you are leaving your computer account/system open to misuse. You should turn this option off in Internet Explorer 7 and Firefox; for details, see [How to Disable Password Saving](#).
- **Change passwords periodically:** Any password can be guessed over time. How long it takes to crack a password is contingent on how strong the password is. The stronger and longer you make it the longer it will take to guess. The time required between password changes is determined by the strength of the password and enforced by the computer system or account being accessed. Users should periodically change passwords for systems/accounts that do not force password changes. Additionally, if you believe one of your passwords has been compromised you should change it immediately.
- **Use different passwords for different types of accounts:** This will minimize the number of accounts that a hacker could gain access to with the same password if compromised.

Minimally you should use a unique password for each of the following categories:

- Signal Sign On accounts such as NetID
 - Other University Systems (PSOS, FRS, PCARD)
 - Personal Financial Accounts
 - Recreational (ie: yahoo, google, hotmail, etc.)
- **Change default password immediately.** Lists of default passwords for devices, applications and accounts are widely available on the Internet. If these passwords are not changed hackers can gain easy access.
 - **Don't write your passwords down unless you then place them in a locked, secured location such as a locked filing cabinet or drawer.**
 - **Don't store passwords in unencrypted files online.** Users who prefer to store this information electronically should use a Password Manager Program such as Password Safe and Password Gorilla. These programs allow users to safely and easily create a secure encrypted username/password list. Then the user only has to create and remember a *single* "**Master Password**". Because this password unlocks and grants access to the owners' entire username/password list it's important to create a strong master password. Once stored, passwords can be copied by double-clicking on them and pasting them directly into the application.
 - **Limit physical access to your computer by locking your computer when you leave.** If you do not lock your system when you go to lunch or leave for the day anyone could sit down at your desk and open files or use your computer to send emails or for other malicious behavior. Microsoft Windows provides an easy way to lock your computer: For XP and Vista press down the windows button -- the one with the Windows logo -- and the "L" button or for Windows 98 and 2000 press and hold down Ctrl-Alt-Del then hit enter.

- **Never provide your password over e-mail or based on an e-mail request.** Emails that request your password or instruct you to go to a Web site link provided in the email to verify your password are most likely fraudulent. Internet "phishing" scams use fraudulent spoofed e-mail messages to entice you into revealing your user names and passwords, steal your identity, and more.

References and Additional Resources:

- [Strong Passwords: How to Create and Use Them](#) by Microsoft
- [Use Strong Passwords](#) by US-CERT
- [Password Safe](#)
- [Password Gorilla](#)
- [UA's Password Construction and Maintenance Guidelines.](#)

For more monthly tips visit:

[University of Arizona's Basic Security Page](#)