



Protect Yourself!

Your password is a primary protective measure against unauthorized access to your information.

As far as the computer is concerned, anybody who knows your UserID and your password, and who uses it to authenticate to the system—**is you!**

EFFECTIVE PASSWORD GUIDELINES

Passwords should be easy to remember... but hard to guess

Passwords should be:

- **Secret—known only to the user.**
- At least eight characters long.
- A mix of upper case, lower case, numbers, and special characters.
- Changed regularly.
- Different for different accounts, and particularly for sensitive information.

Additional Information Security Resources

Sinclair Community College

<http://www.sinclair.edu/departments/infosec/index.cfm>

FTC Consumer Protection Advice

<http://www.ftc.gov/bcp/menu-internet.htm>

US-CERT Security Tips

<http://www.us-cert.gov/cas/tips>

National Cyber Security Alliance

<http://www.staysafeonline.info/>

Microsoft 'Security at Home'

<http://www.microsoft.com/athome/security/default.mspx>



Computer Passwords

Why we need them,
and how to ensure
they are effective!

NOTE: This is intended as a basic guide to illustrate some effective practices and some of the tools available to computer users. *Sinclair Community College does not endorse, or offer technical support for, any of the software or vendors listed in this document.*

Current as of February, 2005
Daniel V. O'Callaghan, Jr., CISSP
Chief Information Security Officer
<http://www.sinclair.edu/departments/infosec/index.cfm>
Sinclair Community College
444 West Third Street
Dayton, Ohio 45402

PASSWORDS...

Keys to
Information Security



Image courtesy of Syracuse University

Computer Passwords

Why we need them, and how to ensure they are effective!

In spite of all the technological advances in information systems since the first PC was introduced in 1981, the combination of a *UserID* (or login ID) and a *password* is still the most common method used to provide access to an individual computer, a network, or other information system resource. When you connect to any information system, the UserID identifies who you say you are, and the password proves you are who you say you are. This is known as *authentication*. The major drawback to this is that as far as the computer is concerned, anybody who knows your UserID and your password, and who uses it to authenticate to the system—**is you!**

Is this a big deal? After all, what attacker cares about your email account? Or maybe you don't have any information stored on your computer that isn't already public knowledge. However, most current hacker attacks are not specifically about your account, but about the access your account has to the systems that will provide resources for a larger or more in-depth attack. While someone reading your email might not seem like much more than an inconvenience or threat to your personal privacy, think of the implications of an attacker gaining access to all the information stored within all the networked or Internet-based information systems you have access to.

In our College environment, federal and state laws—most notably FERPA—dictate how we handle much of the information we use. Who can access information, how this information can be used, and what standards or controls must be implemented are all part of the information security equation. It is very important that each individual who accesses the college information systems has their own account, and that users do not share their account with anyone. Since the password is a primary protection measure, it is imperative that every UserID is protected by an effective password

So what are the characteristics of a 'good' password? The two most important are that it **should be easy to remember but hard to guess** (or otherwise 'crack.')

Some basic rules:

Passwords **should be:**

- Secret—known only to the user.
- At least eight characters long.
- A mix of upper case, lower case, numbers, and special characters.
- Changed regularly.
- Different for different accounts, and particularly for those accessing sensitive information.

Passwords **should not be:**

- The word 'password.'
- Your UserID.
- Words found in a dictionary.
- Any part of your name or institution name.
- Any part of your family members' or pets' names.
- Any part of a number used to identify you (such as Social Security number).
- Your birthday or anniversary.
- Your address or street name

A very effective method for creating a good password is to base it on a sentence or statement you can easily remember. For example, using the sentence *I like to watch Dragons' baseball games* and some simple substitution results in the effective password **I12wD'bg** (**I** like **2** watch **D**ragons' **_**baseball **g**ames).

After creating an effective password, the most critical characteristic becomes secrecy—a password is no longer effective if it has been shared. If you develop the most complex, hard to guess, password ever devised, then write it down and 'post-it' to your monitor (or under your keyboard, or in your pencil drawer)...It's no longer secret or effective.

If you know (or even suspect) that someone else knows your password, you should first determine how they found out and fix the leak, then change your password to a new one. If you suspect your password has been compromised and your account used to access sensitive information or for illegal activity, you should report it immediately.

There is no guarantee that following these techniques will prevent an attacker from accessing any computer system, but by practicing effective password strategies, we strengthen the 'weakest link' in the information security chain and make an attack much more difficult.