

**Enterprise Networking  
Office of Information Technology  
The Ohio State University**

**Password Best Practices**

**March 4, 2004**

**Index**

**1 Overview**

**1.1 Administrative passwords**

**2 Password protection best practices**

**2.2 Storing passwords**

**2.3 Changing passwords**

**3 Password creation best practices**

**3.1 Bad password characteristics**

**3.2 Bad examples**

**3.2 Good password characteristics**

**3.3 Good examples**

**3.4 Good passwords creation tips**

**4 How long does it take to crack passwords?**

**4.1 How passwords are cracked**

**4.2 Estimated times to crack passwords**

**1 Overview**

Students, Faculty, and Staff need to be fully aware of their responsibility to keep their accounts and password as secret as possible

**1.1 Administrative passwords**

User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

## **2 Password protection best practices**

### **2.1 Ways to protect your passwords**

All passwords are to be treated as sensitive, confidential personal information.

Here is a list of "dont's":

Don't reveal a password over the phone to ANYONE

Don't reveal a password in an email message

Don't talk about a password in front of others

Don't hint at the format of a password (e.g., "my family name")

Don't reveal a password on questionnaires or security forms

Don't share a password with family members

Don't reveal a password to co-workers while on vacation

Don't use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Don't use the same password on several computers and/or services as once revealed, it would compromise the security within all the others in one go

Before entering your User ID and password, make sure no one is watching you, to avoid the so-called "shoulder surfing" technique.

Before using your User ID and password on a third-party computer, make sure it is well protected, and free of trojans and key loggers.

### **2.2 Storing passwords**

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

### **2.3 Changing passwords**

Users should change passwords at least once every six months (except system-level passwords which should be changed quarterly). The recommended change interval is every four months.

### **2.4 Password security**

If a university account or password is suspected to have been compromised, report the incident to [security@net.ohio-state.edu](mailto:security@net.ohio-state.edu) and change all passwords.

If someone demands a password, refer them to this document.

## 3 Password creation best practices

### 3.1 Bad password characteristics

Poor, weak passwords have the following characteristics:

The password contains less than eight characters

The password is a word found in a dictionary (English or foreign)

The password is a common usage word such as:

Names of family, pets, friends, co-workers, fantasy characters, etc.

Computer terms and names, commands, sites, companies, hardware, software.

Birthdays and other personal information such as addresses and phone numbers.

Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

Any of the above spelled backwards.

Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

### 3.2 Bad examples

aaa123bbb

abcdefg

76543210

### 3.2 Good password characteristics

Good passwords have the following characteristics:

Contain both upper and lower case characters (e.g., a-z, A-Z)

Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&\*()\_+|~-

=\ {} [] : " ; ' < > ? , . / )

Are at least eight alphanumeric characters long.

Are not a word in any language, slang, dialect, jargon, etc.

Are not based on personal information, names of family, etc.

### 3.3 Good examples

Ona327(sA

@865DapzI

93Sow#-aq

All of these are examples of good passwords, because they fully comply with Password Creation Best Practices; thus containing a mixture of small letters, capital letters, as well as numbers and special characters.

### 3.4 Good passwords creation tips

Use the first letters of a quote, song, etc., for example "Something takes a part of me..." would be 'Stpm'

Join two words, include a number, as well as a special character, for example 'run4life#';

## 4 How long does it take to crack passwords?

### 4.1 How passwords are cracked

The easiest way to crack passwords is to generate character sequences working through all possible 1 character passwords, then two character, then three character, etc. It could start at any specific length password. Theoretically any possible password can be found this way but generally there is not sufficient computing power available to successfully accomplish this.

### 4.2 Estimated times to crack passwords

The table below is calculated by assuming 100,000 encryption operations per second; this is a plausible number for a desktop PC today. Password lengths from 3 to 12 are shown. The numbers at the top, 26 - 94, indicate the number of characters from which the passwords are formed. 26 is the number of lower case letters, 36 is letters and digits, 52 is mixed case letters, 68 is single case letters with digits, symbols and punctuation, and 94 is all the displayable ASCII characters including mixed case letters. The times shown are the times to process the entire set of passwords thus the average time to crack passwords would be one half the listed times.

	26	36	52
3	0.18 seconds	0.47 seconds	1.41 seconds
4	4.57 seconds	16.8 seconds	1.22 minutes
5	1.98 minutes	10.1 minutes	1.06 hours
6	51.5 minutes	6.05 hours	13.7 days
7	22.3 hours	9.07 days	3.91 months
8	24.2 days	10.7 months	17.0 years
9	1.72 years	32.2 years	8.82 centuries
10	44.8 years	1.16 millennia	45.8 millennia
11	11.6 centuries	41.7 millennia	2,384 millennia
12	30.3 millennia	1,503 millennia	123,946 millennia

	68	94
3	3.14 seconds	8.3 seconds
4	3.56 minutes	13.0 minutes
5	4.04 hours	20.4 hours
6	2.26 months	2.63 months
7	2.13 years	20.6 years
8	1.45 centuries	1.93 millennia

9	9.86 millennia	182 millennia
10	670 millennia	17,079 millennia
11	45,582 millennia	1,605,461 millennia
12	3,099,562 millennia	150,913,342 millennia