

Passwords

The use of passwords goes back to ancient times. Sentries guarding a location would challenge for a password.



Select and use a strong password

They would only allow a person in if they knew the password. In modern times, passwords are

used to control access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc.

A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving email from servers, accessing files, databases, networks, web sites, and even reading the morning newspaper online.

Dictionary words and variations of them can be easily guessed by automated password cracking software. Passphrases which are not based on dictionaries or literature are often a better choice than passwords since they are more difficult to crack.



Information Services Department
Information Security Office
55 Lake Avenue North
Worcester, MA 01655

Phone: 508-856-8643
Fax: 508-856-5150
E-mail: ITsecurity@umassmed.edu
Web: <http://www.umassmed.edu/IS/ITsecurity>

Information Security Awareness Series

Password Tips



Security Starts with Awareness for Everyone

October is National Cyber Security Awareness Month

Topic of the Week: Selecting a Password

Did you know that the majority of computer theft can be attributed to the use of weak passwords?



Don't Share Your Password

Despite the name, there is no need for passwords to be actual words; indeed passwords which are not actual words are harder to guess (a desirable property). Note that *password* is often used to describe what would be more accurately called a passphrase.

Passphrase Examples

rsKf0myH&1W2sYU - Raindrops keep falling on my head and I want to steal your umbrella.

wru2axy? - Who are you to ask why?

bWiIso3! - Beware the ides of March!

Password Strength

Studies of production computer systems have for decades consistently shown that about 40% of all user-chosen passwords are readily guessed. *Password strength* is the likelihood that a password can be guessed or discovered by an unauthorized person or computer. Passwords easily guessed are known as *weak* or *vulnerable*; passwords very difficult or impossible to guess are considered *strong*.

Modern password cracking tools can use a list of dictionary terms and phrases, appending and prepending characters and numbers to words in the list, or substituting numbers for letters. Thus choosing a common dictionary term with an adjacent digit or two yields a weak password.

A Strong Password is not

- Personal Information such as your phone number or relative's name.
- Any word in the dictionary, or based solely on such a word spelled backwards.
- A word with letters simply replaced by digits. For example bl0wf1sh.
- Sequential like 12345, or qwerty (i.e. all keys next to each other), or nnnnnn should be avoided.

Strong Passwords

A strong password is as long as possible. Have both upper and lower case letters. The longer the password, the more difficult it is to attack with a brute-force search. Strong passwords:

- Have digits and/or punctuation characters as well as letters
- Are easy to remember so they do not have to be written down
- Are at least eight characters long
- Can be typed quickly so someone else cannot look over your shoulder and learn it

Even if passwords are strong, IS recommends that you change them approximately every six months. Also, never use your University credentials (user name & password) for other online services such as shopping or free e-mail accounts.



Information Services Department
Information Security Office
55 Lake Avenue North

Phone: 508-856-8643

Fax: 508-856-5150

E-mail: ITsecurity@umassmed.edu

Web: <http://www.umassmed.edu/IS/ITsecurity>