# the easiest solution: use a password safe

Password safes save your passphrases or passwords securely, allowing you to save information on your personal computer without giving away private information inadvertently. They can also generate random passphrases for each of your accounts.

These password safes store all of your passphrases in a single account, which has a master passphrase you need to remember. Password safes allow you to use truly random combinations in all other passphrases, making them more difficult for malicious users or bots to crack. Two examples of these services are LastPass and Password Gorilla.

#### change your passphrase regularly

Passphrases should be changed:

- Whenever a malicious program such as a virus is detected or a machine is compromised
- Whenever leaving a job or starting a new one
- From any default passphrases
- If they are shared with anyone at any time

Content used with permission from Rochester Institute of Technology. Updated 8/19/15.



If you have forgotten your passphrase or believe it has been compromised, contact the **UBIT Help Center:** 

716-645-3542 Email: ubithelp@buffalo.edu

## get informed

Visit the UBIT website to read the security standards, access security tools and software, or find out more ways to protect yourself.

UB INFORMATION SECURITY OFFICE www.buffalo.edu/ubit/security

sec-office@buffalo.edu



(716) 645-6997

**UB** Information Technology University at Buffalo

DIGITAL SELF DEFENSE:

#### how to create a secure passphrase

Passphrase - the next generation in passwords!



## what is a secure passphrase?

A secure passphrase is the next generation in passwords. It uses a short phrase instead of a single word, making it more difficult for someone else to guess or use.

It should be virtually impossible for others to guess, and not contain or be based on personal information. Passphrases should never be written down or given to anyone else.

## what should I avoid?

There are many ways people try to make their passphrases easier to remember. Password cracking programs look for the most common passwords first.

Passphrases should NOT:

- Contain your UBITName
- Be the same as other passphrases you are currently using (including non-UB services)
- Be a single word, forward or backward, from an English or foreign dictionary
- · Contain more than three sequential characters on a keyboard (ex: gwerty or 1234)
- Contain more than two consecutive repeating characters (bbbb2bbb)
- Be all numbers such as birth or anniversary dates (ex: 011551)
- Be shared with anyone for any reason

# how do I create an easy to remember passphrase?

Here are three simple ways to construct a secure, easy to remember passphrase:

- 1. Create a passphrase by taking a short phrase and:
  - Change the capitalization of some of the letters
  - Replace some of the letters with numerical and symbolic substitutions (\$ for S, 8 for B)
  - Misspell or abbreviate some words
- (E.g., the phrase "iced tea is great for summer" becomes "!cedTisgr84\$umm3R".)

2. Choose several shorter words and add some numbers in the center, then change the capitalization and substitute symbols for letters. (E.g., the phrase "book 451 Bradbury" becomes "bO()K451BR^Dbury".)

3. Choose a memorable quote or phrase and use only the first letter from each word. Vary the capitalization.

Also include numbers and symbols, either as substitutions for letters or as a replacement for a full word. (E.g., Wayne Gretzky's "You will always miss 100 percent of the shots that you never take" becomes "ywAM100%ot\$tyN+".)

Requirements for passphrases can be found at: http://www.buffalo.edu/ubit/password-safety

HINT: You can also use a password safe, a program that generates and stores random, secure passwords.

#### protect your passphrase

There are several different ways someone can acquire your passphrase:

- Cracking: Password cracking programs are • designed to guess the most common passphrases first. Most current programs can make over one million crack attempts per second.
- Malware: Password stealers and keyloggers are often packaged with viruses and spyware. Always run up-to-date anti-virus.
- Social Engineering: Never give away your passphrase to anyone, even someone claiming to work for a help desk.
- Phishing: Universities and companies will never ask you to confirm your passphrase through email, so don't click on links in an email asking you to do so. Type the URL into a Web browser manually.

#### why use a secure passphrase?

If someone cracks your passphrase, they can:

- Obtain your personal information, which can lead to identity theft
- Gain access to your email account to read and send email
- Access MyUB, HUB Student Center or other services
- Access confidential UB information on the university's network
- 103030300300300303010 J Gain information about your registered computers at UB and register their own on your UB account.

www.buffalo.edu/ubit/security