



Take a second to be secure.

The Security Minute

A communication of the Longwood University Information Security Office

Read *The Security Minute* Online: www.longwood.edu/infosec

June 2008



What is a... dictionary attack

A dictionary attack is a method of trying to obtain access to a system by using a list of words from several common languages and simple variations on those words to try to guess a password. Using a variety of characters (uppercase, lowercase, numbers and symbols) and longer passwords make dictionary attacks more difficult.



Security Spotlight

Need to change your password?

Use CYPHIR (Change Your Password or Have it Reset).

Start here:

https://www2.longwood.edu/cyphir/cyphir_welcome.asp

Shaking it Up: Changing Your Password Regularly

The towering redwood trees of California have been known to survive for 2000 years as they resist the threats of insects and fire. Unfortunately your password is more like a marigold, the annual flower that lasts just one season.

Overtime your password becomes more vulnerable to being compromised. The longer you have use been using a particular password the greater the chance that someone else also knows your password. However, when you change your password that individual will no longer be able to access your account.

How do others get your password?

- **Keyloggers** – Keyloggers are malicious programs that record everything you type and can be used to discover user names, passwords, bank account numbers and other confidential information. Even if the computers you access at home and at work are protected from some keylogging programs by antivirus software, your password may be at risk if you ever utilize public computers such as the ones in hotel lobbies which are often much less secure.
- **Intercepted Wireless Traffic** – Like public computers, using wireless access provided in public places, such as coffee shops or airports, may also put your password at risk. Wireless traffic is not as secure as wired traffic and passwords may be intercepted.
- **Phishing** – These e-mails that appear to be from a legitimate institution, but are actually from a scammer looking for account details are another way that passwords can be stolen.
- **Shoulder Surfing** – Passwords can be obtained from people trying to watch you type your password in. Unfortunately many times password stealing, such as through shoulder surfing, is made easier by the selection of easy to guess passwords. Names of family members, vacation spots or sports teams may be easy to guess, especially if your desk or office also contains references to those aspects of your life.

In addition to the required password change schedule you may need to change your password if at any time you believe it may have been obtained by someone else. Such as:

- If you are suspicious of a public computer you have accessed
- If you believe that public wireless access you used may not have been trustworthy
- If you believe you may have responded to a phishing e-mail
- If you observe someone acting suspiciously as you type your password
- If you believe your password may be easy to guess

Security Tip: *If you must write down your password then protect that piece of paper like you would protect your credit card!*



The Security Minute is a monthly publication aimed at raising awareness of information security related issues and concerns. If you have any questions regarding the newsletter, please contact Melissa Short at 434-395-2034 or shortmj@longwood.edu.