



# The Security Minute

Take a second to be secure.

A communication of the Longwood University Information Security Office

Read *The Security Minute* Online: [www.longwood.edu/infosec](http://www.longwood.edu/infosec)

## Passwords: Making Passwords Difficult to Guess

Choosing a long password with a variety of characters can protect your password from hackers who attempt to crack your password with automated programs. However, such passwords may still be vulnerable to guessing by those who know you or target you for a scam.

If you have a web site, blog, Facebook or MySpace profile or other online profile make sure that none of the passwords you choose (for your LancerNetID, bank, social networking account, etc.) can be easily guessed from the information available about you online.

**Example:** If in your blog you write extensively about your cat named Mittens your bank password should not be *Mittens1*.

Remember that the rules of good password maintenance don't just apply to your LancerNet ID. Long, complex, regularly changed, difficult to guess passwords are equally important on non-University systems. Consider the implications of someone correctly guessing the password to your Facebook profile or blog. Could someone post reputation damaging information about you as a result? If someone guessed the password to your blog would they also then have the password to another online service you use, like online banking.

Using different passwords on different accounts is also important for ensuring that your passwords are always difficult to guess. The University's Minimum Password Standards associated with University Policy #6119: Password Management actually requires users to only use the LancerNet ID and password for Longwood systems and services and to create a different username and password for external services.

January 2009



### What is scareware?

Scareware is a term for fake security (antivirus) software that users may be prompted to buy and/or install because of a bogus advertisement that claims the computer is infected.



## The Key to a Good Password: Be Mysterious

Don't select passwords that friends, acquaintances, enemies or scam artists can easily guess.

## Make Sure Your Secret Questions Are Difficult to Guess Too!

Not only should your password be difficult to guess, the answer to your secret questions should also be difficult to guess. Many online services will let you choose secret questions that you will be asked in the event that you forget your password. If one of your secret questions is where were you born and your personal web site says "born and raised in Farmville, VA" then you could have just given away access to your account. This is how former vice presidential candidate Sarah Palin's personal e-mail account was hacked during the fall. A hacker correctly answered her secret questions which included a question about where she met her husband, which was a commonly known, easy-to-find fact.

To create stronger secret questions:

- Lie or be very detailed in your answers
- Consider how much information you really want to share in your online profiles
- Select secret questions for which you have not previously publicized the answer



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](mailto:shortmj@longwood.edu).