



SANS OUCH!

SANS Institute Security Newsletter for Computer Users

February 2010

Check out the new OUCH! Security Information Service at:

<http://www.sans.org/newsletters/ouch/updates/>

In This Issue:

- What's your Password IQ?
- Patches and Updates Roundup

[Editor's Note: (Wyman) Your password is more than just a key to your computer or online account. If your password falls into the wrong hands, a Bad Guy can impersonate you online easily, tinker with your bank accounts, sign your name to online service agreements or contracts, engage in financial transactions, or change your account information. Find out how much you know about safe password practices by taking our quick quiz.]

What's your Password IQ?

#1. How often should you change your password?

- a) Every 30 days
- b) Every 60 days
- c) Every 90 days
- d) When IT tells you to

Answer: (a) – And the more often you replace your strong password with another strong password, the better. What's a “strong” password? Read on.

#2. One of your co-workers is working on a critical report this weekend and needs access to some of your files. How should you give her your password?

- a) Send it in an email message
- b) Call her on the phone and tell her the password
- c) Don't give it to her or anybody else
- d) Write it on a piece of paper, seal it in an envelope, and mail it to her

Answer: (c) – If she needs access to your files, call your IT department and ask them to give her access without the use of your password.

#3. What is the most common (and so the weakest) password used in 2009?

- a) password
- b) 123456
- c) qwerty

d) abc123

Answer: (a) – Actually, the list is in order, according to *PC Magazine*.^{*} If you are using these passwords or anything like them, you might as well just give people access to your computer or your bank account.

#4. What characters should you use in a password to make it strong?

- a) Letters only
- b) Numbers only
- c) Letters and punctuation
- d) All of the above

Answer: (d) – The more complex a password is, the harder it is for a person to guess it. Some systems and websites may not allow you to use all of the punctuation symbols, but most allow some of them.

#5. How long should a strong password be?

- a) Five characters
- b) Eight characters
- c) As long as possible
- d) Size doesn't matter

Answer: It depends! For technical reasons, a *minimum* length of 8 characters is recommended. But not all eight-character passwords are equally strong. For example, “football” wouldn't be hard to guess, but guessing the 8 characters of 7xkM*vh\$ presents a real challenge.

#6. Now that you are an expert, choose the strongest password from this list:

- a) Mickey.Mouse
- b) M1ck3y.m0u53
- c) 3.1416**
- d) Ad@46-Hiz
- e) Aristotle

Answer: (d) – (a) is obviously easy to guess, even though it's long enough; (b) is “hacker-speak” for Mickey Mouse – a bad idea; (c) contains no letters – and it's the approximate value of Pi; and (e) is a proper name.



Strong Password Checklist:

- ✓ at least 8 characters
- ✓ at least one number
- ✓ at least one uppercase and one lowercase letter
- ✓ at least one symbol (examples: &, !, @, #, \$, ^, *)
- ✓ no proper names or words (English or otherwise)
- ✓ no personal information, like your SSN, phone number, or date of birth
- ✓ no repeating characters
- ✓ no easy-to-guess patterns like 123qwerty
- ✓ no well-known mathematical values (like Pi) or equations (E=mc²)

Tips!

- Treat passwords like your toothbrush: Choose a good one and replace it regularly.
- Change your passwords at least every 30 days.
- Use a passphrase. Choose an easily remembered phrase like “Liberty and Justice Forever” and use the first one or two letters of each word with some punctuation and numbers in between. Example: Li.an1Ju*Fo.
- Use a password pattern. Pick a starting point on the keyboard, trace out an easily remembered pattern, and add some twists. Example: The eight-character pattern 1qscvhU* describes a “V” on your keyboard starting with the number 1 key, with the added twists of an uppercase U and an asterisk.
- Use a password manager. If you use Firefox, for example, you can have your browser remember your passwords. Then be sure to set a strong master password in Firefox to protect your “remembered” passwords. <http://www.firefoxfacts.com/2008/05/08/how-to-use-a-master-password/>.
- Other versatile, no-cost or low-cost password managers include Roboform (<http://www.roboform.com/>) and KeePass (<http://keepass.info/>).

More Information:

- *<http://www.pcmag.com/article2/0,2817,2113976,00.asp>
- <http://www.microsoft.com/smallbusiness/resources/technology/security/5-tips-for-top-notch-password-security.aspx>
- <http://support.apple.com/kb/HT1506>

Patches and Updates

Windows & PC Office: <http://update.microsoft.com> and <http://www.microsoft.com/security/updates/bulletins/201001-OOB.aspx>

OS X: <http://support.apple.com/kb/HT1338>

Mac Office: <http://www.microsoft.com/mac/help.msp?CTT=PageView&clr=99-0-0&ep=7&target=ffe35357-8f25-4df8-a0a3-c258526c64ea1033>

iPhone/iPod: <http://support.apple.com/kb/HT1414>

iPod: <http://support.apple.com/kb/HT1483>

Windows Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows>

OS X Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Macintosh>

Flash Player: <http://get.adobe.com/flashplayer/>

Firefox: <http://www.mozilla.com/en-US/firefox/update/>

Safari: http://www.apple.com/downloads/macosx/apple/application_updates/safari.html

Opera: <http://www.opera.com/>

Chrome: <http://googlechromeupdate.com/updates.html>

Java: <http://www.java.com/en/download/manual.jsp>

iTunes: <http://www.tuaw.com/2009/09/22/itunes-9-0-1-now-in-software-update/>

Symantec: <http://service1.symantec.com/SUPPORT/sharedtech.nsf/docid/2002021908382713>

Norton:

http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=n95

McAfee: http://www.mcafee.com/apps/downloads/security_updates/dat.asp

Kaspersky: <http://www.kaspersky.com/avupdates>

Sophos: <https://secure.sophos.com/support/updates/>

Panda: <http://www.pandasecurity.com/homeusers/downloads/clients/>

BitDefender: <http://www.bitdefender.com/site/view/Desktop-Products-Updates.html>

Microsoft Security Essentials:

<http://www.microsoft.com/security/portal/Definitions/HowToMSE.aspx>

Copyright 2009, SANS Institute (<http://www.sans.org>)

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Alicia Beard, Alan Paller.

Email: OUCH@sans.org

Download the formatted version of the OUCH! at <https://www.sans.org/newsletters/ouch>

Permission is hereby granted for any person to redistribute this in whole or in part to any other persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product. We request that redistributions include attribution for the source of the material.
