

# Medical Office Systems, LLC

## February 2010 Newsletter

---

### February Topics

**A good password...** is not a word. Find out how to create a strong passphrase.

**More about “phishing”...** learn about the rising incidence and sophistication of computer attacks via email.

If you have any questions about passwords or email security, please call me at 630-852-1736 or 630-373-7429.

### Get the Newsletter by Email!

Visit my website [www.MedOfficeSystems.com](http://www.MedOfficeSystems.com) and sign up to get the newsletter delivered to your email in-box.

---

### A Good Password

Passwords are the single most important facet of computer security. Your password is the last line of defense against unauthorized use of your computer, hacking activity, and / or data theft. If your password is revealed, discovered, or guessed, the net effect is your account has **no** security.

Whether your account is on your computer, or is an online account such as email, banking, or other confidential source, there are a few very basic guidelines to always follow, and some guidelines on how to create a strong, un-guessable password.

#### **Basic Guidelines:**

1. Don't leave passwords on yellow sticky notes on your monitor, keyboard or other location near your computer. Putting it under the keyboard is not going to fool anyone! If you must write it down, put it in a safe location away from your computer.
2. The temptation to give out your password may be hard to resist, especially when you are rushed at work and trying to get a task or job done. Resist the temptation to give your password to an employee or co-worker. Pretend your password is your credit card, and you just gave it to a stranger!
3. Be aware of email or phone scams – especially in large corporations. Callers or email senders may pretend they are “the IT department”. They say they need to reset your password, or your account will be locked forever, cancelled, or other dire circumstance.
4. Don't use easy to guess passwords, like your last name, “123”, “ABC” “qwerty” etc.

#### **Strong Passwords:**

I don't like using the term “password”. I prefer to think more in terms of “passphrase”, ie: a long password.

#### **A strong password is:**

- a long password, eight (8) characters minimum, longer is better
- a mix of numbers, letters, and symbols
- does not use words that are in the dictionary
- does not use personally identifiable names, nicknames, pet's name, etc.

**Why?** You are trying to foil both human and computer-based password guessers. Humans will try likely combinations of words, names, etc. that can be known about you. An example: the situation with a Vice-President candidate's online email being “hacked” last fall was in reality an easily guessed password, and not due to any sophisticated hacking methods.

[continued]

Reprint permission granted, provided the following appears on each page:  
Copyright © 2009, Medical Office Systems, L.L.C. - [www.medofficesystems.com](http://www.medofficesystems.com)

Phone: 630-852-1736

[john@medofficesystems.com](mailto:john@medofficesystems.com)

Fax: 630-214-4565

### A good password continued...

On the other hand, an automated password-guessing program can check an entire dictionary's list of words in just a few minutes. No sophistication is required, just brute force: hundreds and thousands of guesses and combinations of common passwords per minute until it gets one right.

### How to build a Strong Password:

Passwords should be easy to remember yet complicated enough not to be guessed. You'll need at least two things you know well and a little creativity.

**Example 1:** I could use an old license plate, ABH985 – I remember it well, yet it is no longer associated with me. I take that, and add the symbols (# and +) at the start and middle resulting in: #ABH+985.

**Example2:** Start with two words, in this case I am using "fish" and "freight". I substitute the dollar symbol (\$) for the "s" in "fish" and substitute the number "8" for "eight" in "freight", finally I put the "@" symbol between the two words:

Example	Before	After
#1: just add symbols:	ABH985	#ABH+985
#2: be creative with symbols, numbers:	fish freight	fi\$h@fr8

Keep in mind that upper and lower case matters, so if you choose to mix upper/lower case, remember that also. I have added links on my website to Microsoft's enhanced password schemes and password rating web page along with the Sophos "*Top 20 passwords you shouldn't be using*" article. The link to the articles is below.

## More About Phishing

The recent flap between Google and China about government-sponsored hacking is a reminder to all of us to be aware of so-called "phishing" and "malware" attacks. The hacking began with a hidden link in a scam email (phishing) that enticed certain targeted human-rights activists to login at a fake Gmail website. The fake login page was actually "harvesting" the user ID's and passwords. The harvested logins were in turn used by the hackers to legitimately login to Gmail and spy on the user's email. Once logged in, the hackers then tried to launch further attacks on Google itself and spread malware from within the email environment.

I have a detailed example on my website of a similar attack via phishing email I received. It appears like it came from Vonage, an Internet phone company. It is quite realistic, and purported to warn me that my account is locked. Since I do not now, and have never owned a Vonage account, I did not have to worry. I decided to play along, and recorded each step of the process. Quite an interesting exercise, the perpetrators went to great lengths to make the fake site look realistic, even to the point of registering a similar-looking web address. I posted a 3-page slide show of screen captures from this phishing attack on my website, see the link below.

As always, if you have questions or need assistance, please call me. There are many strategies and products I can recommend to help reduce or eliminate security threats received via the Internet.

Link to More Articles: [http://www.medofficesystems.com/newsletter\\_tips.htm](http://www.medofficesystems.com/newsletter_tips.htm)

Reprint permission granted, provided the following appears on each page:  
Copyright © 2009, Medical Office Systems, L.L.C. - [www.medofficesystems.com](http://www.medofficesystems.com)