

### Social Media Users Beware: Logins and Passwords

**How did my email get hacked?** ...is a question I frequently get from clients, friends and family members. The answer is not one you would expect. It is now less likely that your email will be hacked by virus-based attacks, and more likely through social media website attacks. Although you cannot fully protect yourself while using social media sites, you can make it harder to be a victim of hacking.

Missed or lost a newsletter? You can always get back issues in Adobe PDF format online at my website - [www.MedOfficeSystems.com/newsletter\\_tips.htm](http://www.MedOfficeSystems.com/newsletter_tips.htm)

---

### Social Media Users Beware: Logins and Passwords

If you've had your email ID hacked and have suffered the embarrassment of having your address being used to spread spam, chain letters or viruses, you rightly wonder how this happened. If you are a frequent social media user, it is very likely that your use of websites such as Facebook, MySpace, Twitter, and others is the culprit.

Let's use Facebook for our example. Why Facebook? Well, because it's so wildly popular, and popularity draws a crowd... of hackers. Just ask Microsoft – the biggest player is also the biggest target. Facebook's lack of security features is typical of most social media websites. Collectively, social media sites lack even the most rudimentary security measures and protections. Notably absent from this list is LinkedIn – while not a security fortress, it at least has secure logins.

#### Reason #1: No SSL "Lock" while logging in

That little "lock" icon you see in your browser while using corporate, banking, investing, medical, and other secure websites is absent from Facebook. Small detail, but large implications – your user ID and Password are not encrypted, and therefore easily read by anyone with modest tech skills. A high-school kid with a laptop and one of the many free internet protocol analyzers can read the traffic passing through a public WIFI connection and grab your email address and password in seconds. If Facebook had a secure website, the same login would look like gibberish to the high school kid. Not having a secure login is like sending a confidential message via a postcard: your letter carrier could not read the message if it were in an envelope, but the postcard is open season.

#### Reason #2: Weak Passwords

This is a two-phase problem – 1) many people select weak passwords... and 2) Facebook allows it. There should be some effort by Facebook to enforce strong passwords. A weak password is defined as easy to guess. Easy to guess means:

1. It contains any information about you:
  - a. any part of your birthdate
  - b. your initials
  - c. only has letters or only numbers
  - d. your name... and so on.
2. Or the password has any of the following characteristics:
  - a. any word found in the dictionary
  - b. shorter than 8 characters
  - c. any data that can be traced to you: family names, pets, street address, school, phone number, etc.

## **Why should I care? Facebook is all about being open, so what?**

You absolutely should care, especially if you use the same password for Facebook as you do for your personal or work Email. Or your online banking. Or your computer login. Or anything else you care to keep private. Collateral damage to friends and associates ensues when your email or Facebook account is hacked, all your contacts are vulnerable to malicious content in any postings made or emails sent “as if” it was you.

## **Example #1: Weak Password + Public WIFI + Used on too many sites = empty bank account**

Joe Smith used his work email ([j.smith@reallybigcorp.com](mailto:j.smith@reallybigcorp.com)) to sign up for Facebook, and also used it for his online bank. Joe uses his work password of jsmith123 because it's easy to remember. One morning, while using the public wifi at his favorite coffee shop, Joe logs into Facebook to see what's up. Less than an hour later, Joe gets a call from a friend about the weird postings Joe put on Facebook about a new pharmaceutical and how great it is. Joe says he did no such thing, but will check it out later. At lunch, he logs onto his online bank, but the password does not seem to work. Joe calls the bank tech support and is told he already changed it this morning, and there was a large withdrawal. Uh-Oh.

## **Example #2: Good Password, but easy to guess = hacked anyway**

Linda used her AOL email to set up her Facebook account, and chose 'DGhs1989' as her password. That is a pretty good password: it has upper/lower case letters, is not a word, and has numbers in it, and it eight digits long. However, on her Facebook profile, she lists Downers Grove High School as her alma mater, and she graduated in 1989. Oops.

## **Guidelines:**

The easiest thing to do is quit Facebook... but that's not reality for many people. If you are going to use Facebook, it's essential to step up your security practices:

1. Don't use your work email or password
2. Don't use the same password for Facebook that you use anywhere else
  - a. Make a new password for Facebook only.
3. When creating a new password, make it hard to guess
  - a. Don't use any personal information that can be known or guessed
  - b. Use a mix of:
    - i. upper/lower case letters
    - ii. numbers
    - iii. symbols ( + - \* \$ # ! % & \_ )
4. If you have trouble, or want to check if your password is strong, try the Microsoft password rating web page: <http://www.microsoft.com/protect/fraud/passwords/create.aspx>
5. A more aggressive approach: Create a new email address and password just for Facebook
  - a. Use a free email provider such as Gmail, Yahoo, or MSN - they all use safe login procedures.
  - b. Change your email address on Facebook to the new “facebook-only” email / password.

## **Summary:**

Even though there are security flaws on most social media websites, you can take steps to protect yourself. Make your password hard to guess. Never use the same password on both secure and insecure sites. A more aggressive strategy includes creating a new email address and password only to be used with social media sites.

Please call me if you have any questions about passwords, logins, or social media questions. Keep your ID safe!