**Security For Your Business**

# Protecting yourself, your clients, & your business online is a serious matter.

#### **5 tips for top-notch password security| Microsoft Small Business Center**

Kim Komando writes about workplace technology and security issues. She's the host of the nation's largest talk-radio show about computers and the Internet, and writes a syndicated column for more than 100 Gannett newspapers and for USA Today. Find Kim's show on the radio station nearest you, and send an e-mail to subscribe to her free weekly e-mail newsletter.

By Kim Komando

Whether it's a few PCs or hundreds on your network, there's one thing that can separate your system from being compromised: a great password.

Why? Hackers want access to anything and everything. If they can guess your user name and password, you might as well have given them your wallet and the keys to your building.

Before we talk about what makes a good password, let's begin with the first of five things to know and practice in using passwords.

**1. Don't be complacent: Attacks can and do happen.**

Hackers are a devious bunch and will stop at nothing to get into your network and files. They use three different methods to get to you: brute force, dictionary attacks, and social engineering.

Brute force is the most time-consuming method. Basically, it involves a program that tries every combination of letters, numbers, and keyboard characters to guess your password. It starts with trying every character, then tries two-character combinations, and so on.

The longer the password is, the exponentially more difficult it becomes to crack. According to George Shaffer, a password expert, a password that is eight characters in length and utilizes lower- and upper-case letters, numbers, and keyboard characters won't be cracked for two years. This underscores the importance of being as random as possible when choosing your password. (More tips from Shaffer on creating passwords are available at www.geodsoft.com/howto/password).

Another method of attack is through the use of custom dictionaries. These dictionaries are filled with words and names, but also number and letter combinations, such as 11111 and abc123. Simple passwords such as "duke" or "ilovemydog" can easily be guessed.

The third and most effective method of attack is social engineering. This involves someone with criminal intent soliciting a password directly from a user. Many people divulge their passwords to co-workers and strangers without even realizing it.

For example, most small businesses don't have a dedicated information-technology staff. A hacker posing as someone from your company's Internet service provider could call in and get an unsuspecting employee's password by "testing the service." The hacker might request the employee's user name and password to log in and test the connection from the ISP's end. If the hacker sounds authoritative and legitimate enough, your whole network could be compromised.

If your business rents space in a larger facility, strangers probably roam the hallways unnoticed. A few innocent questions or a watchful eye can be disastrous.

**2. Know what makes for a bad password**.

Because the attacks described above are becoming increasingly more common, you don't want to use anything in your password that's personal and easy to guess. Keep in mind the following don'ts:

Don't use only letters or only numbers.

Don't use names of spouses, children, girlfriends/boyfriends or pets.

Don't use phone numbers, Social Security numbers or birthdates.

Don't use the same word as your log-in, or any variation of it.

Don't use any word that can be found in the dictionary — even foreign words.

Don't use passwords with double letters or numbers.

Some of the worst passwords are: password, drowssap, admin, 123456, and the name of your company or department. Finally, never leave it blank. That's a surefire way to let the bad guys into your system.

3. Get proficient at creating good passwords.

A good password is one that is easy to remember but difficult to guess. That sounds like a paradox, but it's really not.

There are a couple of different ways to create difficult-to-crack passwords. One is substituting letters with characters and numbers. To make it easier on yourself, try to use numbers and characters that resemble the letters they are replacing.

For example, you would never want to use the word "password" as your password. If you change it to p@7sw0rd!, you've got something that would take some time to crack but is fairly simple to remember.

Another method is to use the first letters of the words in a favorite line of poetry or a verse of song. "Hail, hail the lucky ones, I refer to those in love" becomes "H,hTL0,IR2t1L."

The best passwords are at least eight characters in length and use a combination of numbers, keyboard characters and upper- and lower-case letters. The longer your password is, the longer it will take someone (or more likely, some program) to crack it.

4. By all means, safeguard your password.

At first, it may be difficult to remember your password. Did you substitute an "i" with a "1" or did you use a "1" to represent "L?" Most people will want to write the password on a piece of paper and place it underneath their keyboard or mouse pad. Or worse, they'll stick the password right on their monitor.

To help remember the password, use it immediately. Then log in and out several times the first day. Just don't change it on a Friday or right before leaving for vacation. You could write it out several times on a piece of paper. This helps record it in your mind. Just be sure to shred the paper when done.

Invariably, there may come a time when a password has to be shared. Let's say an employee is out of town to give a presentation but left the PowerPoint file on his desktop. You will have to get his user name and password to access that file. After you open the file, change the password and give him the new password upon his return. Then, as soon as the person gets back into the office, have him change the password again. Yes, it's a lot of work but well worth it.

5. Change your password often—as in several times a year.

Your network administrator can force your employees to change their password every so often. Microsoft recommends having users change their passwords every 30 to 90 days, but encourages you to go with the smaller number. I think 30 days is a reasonable number here. You always want to side with caution when it comes to sensitive information.

If you're like me, you allow your employees to do light surfing at lunch and on breaks. Encourage your employees to change their passwords to personal Web sites as well—such as to banking, Internet e-mail accounts, shopping sites, and so on. Advise them not to use the same password for all of their sites. A particularly good hacker can cause personal financial ruin by gaining access to one username and password.

Juggling all of these passwords is not easy. You might want to consider a program that can do all of this for you. Account Logon (www.accountlogon.com) and Roboform (www.roboform.com) are two well-reviewed password management programs; both offer free versions.

Now the following is an eerie thought — but it's something that must be taken into consideration.

What if you or your network administrator dies?

Well, if you've used best practices when creating a password, nobody else knows your password. And it's so complex that it could take months to crack the code or money to buy the right software for the job. Just in case, you might consider keeping a copy of all passwords in the company's safe. As for your personal passwords, keep them stowed away somewhere along with your will.

# In another alarming example, the report highlights Active Directory's policy of password complexity, which states that a password is required to have a minimum of eight characters and three of the five character types (Lower Case, Upper Case, Numbers, Special, Unicode). Guess what meets those requirements? "Password1", "Password2", and "Password3", the first being the most widely used across the pool of two million passwords studied in the report.

**The top 10 passwords identified by the study were:**

**Password1  
welcome  
password  
Welcome1  
welcome1  
Password2  
123456  
Password01  
Password3  
P@ssw0rd**

**Variations of "password" made up about 5% of passwords and 1.3% used "welcome" in some form.**

**How I’d Hack Your Weak Passwords**

John Pozadzides – December 2010

Internet standards expert, CEO of web company iFusion Labs, and blogger John Pozadzides knows a thing or two about password security—and he knows exactly how he'd hack the weak passwords you use all over the internet.

Note: This isn't intended as a guide to hacking \*other people's\* weak passwords. Instead, the aim is to help you better understand the security of your own passwords and how to bolster that security. We originally published this piece back in March, but in light of our recent security breach, it seemed more applicable than ever.

**If you invited me to try and crack your password, you know the one that you use over and over for like every web page you visit, how many guesses would it take before I got it?**

**Let's see… here is my top 10 list. I can obtain most of this information much easier than you think, then I might just be able to get into your e-mail, computer, or online banking. After all, if I get into one I'll probably get into all of them.**

**1.     }Your partner, child, or pet's name, possibly followed by a 0 or 1 (because they're always making you use a number, aren't they?)**

**2.      The last 4 digits of your social security number.**

**3.      123 or 1234 or 123456.**

**4.      "password"**

**5.      Your city, or college, football team name.**

**6.      Date of birth – yours, your partner's or your child's.**

**7.      "god"**

**8.      "letmein"**

**9.      "money"**

**10.   "love"**

Statistically speaking that should probably cover about 20% of you. But don't worry. If I didn't get it yet it will probably only take a few more minutes before I do…

Hackers, and I'm not talking about the ethical kind, have developed a whole range of tools to get at your personal data. And the main impediment standing between your information remaining safe, or leaking out, is the password you choose. (Ironically, the best protection people have is usually the one they take least seriously.)

One of the simplest ways to gain access to your information is through the use of a Brute Force Attack. This is accomplished when a hacker uses a specially written piece of software to attempt to log into a site using your credentials. Insecure.org has a list of the Top 10 FREE Password Crackers right here.

**So, how would one use this process to actually breach your personal security? Simple. Follow my logic:**

}You probably use the same password for lots of stuff right?

}Some sites you access such as your Bank or work VPN probably have pretty decent security, so I'm not going to attack them.

**However, other sites like the Hallmark e-mail greeting cards site, an online forum you frequent, or an e-commerce site you've shopped at might not be as well prepared. So those are the ones I'd work on.**

So, all we have to do now is unleash Brutus, wwwhack, or THC Hydra on their server with instructions to try say 10,000 (or 100,000 – whatever makes you happy) different usernames and passwords as fast as possible.

Once we've got several login+password pairings we can then go back and test them on targeted sites.

}**But wait… How do I know which bank you use and what your login ID is for the sites you frequent? All those cookies are simply stored, unencrypted and nicely named, in your Web browser's cache.** (Read this post to remedy that problem.)

And how fast could this be done? Well, that depends on three main things,**the length and complexity of your password, the speed of the hacker's computer, and the speed of the hacker's Internet connection.**

Assuming the hacker has a reasonably fast connection and PC here is an estimate of the amount of time it would take to generate every possible combination of passwords for a given number of characters. After generating the list it's just a matter of time before the computer runs through all the possibilities – or gets shut down trying.

**Pay particular attention to the difference between using only lowercase characters and using all possible characters (uppercase, lowercase, and special characters – like @#$%^&\*).   Adding just one capital letter and one asterisk would change the processing time for an 8 character password from 2.4 days to 2.1 centuries.**

Remember, these are just for an average computer, and these assume you aren't using any word in the dictionary. If Google put their computer to work on it they'd finish about 1,000 times faster.

Now, I could go on for hours and hours more about all sorts of ways to compromise your security and generally make your life miserable – but 95% of those methods begin with compromising your weak password. So, why not just protect yourself from the start and sleep better at night?

Believe me, I understand the need to choose passwords that are memorable. But if you're going to do that how about using something that no one is ever going to guess AND doesn't contain any common word or phrase in it.

**Here are some password tips:**

1.  Randomly substitute numbers for letters that look similar. The letter ‘o' becomes the number ‘0′, or even better an ‘@' or ‘\*'. (i.e. – m0d3ltf0rd… like modelTford)

2.      Randomly throw in capital letters (i.e. – Mod3lTF0rd)

3.      **Think of something you were attached to when you were younger, but DON'T CHOOSE A PERSON'S NAME! Every name plus every word in the dictionary will fail under a simple brute force attack.**

4.      Maybe a place you loved, or a specific car, an attraction from a vacation, or a favorite restaurant?

5.      You really need to have different username / password combinations for everything. Remember, the technique is to break into anything you access just to figure out your standard password, then compromise everything else. This doesn't work if you don't use the same password everywhere.

6.      Since it can be difficult to remember a ton of passwords, I recommend using Roboform for Windows users. It will store all of your passwords in an encrypted format and allow you to use just one master password to access all of them. It will also automatically fill in forms on Web pages, and you can even get versions that allow you to take your password list with you on your PDA, phone or a USB key. If you'd like to download it without having to navigate their web site here is the direct download link. (Ed. note: Lifehacker readers love the free, open-source KeePass for this duty, while others swear by the cross-platform, browser-based LastPass.)

7.     Mac users can use 1Password. It is essentially the same thing as Roboform, except for Mac, and they even have an iPhone application so you can take them with you too.

8.     Once you've thought of a password, try Microsoft's password strength tester to find out how secure it is.

By request I also created a short RoboForm Demonstration video. Hope it helps…

**Another thing to keep in mind is that some of the passwords you think matter least actually matter most. For example, some people think that the password to their e-mail box isn't important because "I don't get anything sensitive there." Well, that e-mail box is probably connected to your online banking account. If I can compromise it then I can log into the Bank's Web site and tell it I've forgotten my password to have it e-mailed to me. Now, what were you saying about it not being important?**

Often times people also reason that all of their passwords and logins are stored on their computer at home, which is safe behind a router or firewall device. Of course, they've never bothered to change the default password on that device, so someone could drive up and park near the house, use a laptop to breach the wireless network and then try passwords from this list until they gain control of your network — after which time they will own you!

Now I realize that every day we encounter people who over-exaggerate points in order to move us to action, but trust me this is not one of those times. **There are 50 other ways you can be compromised and punished for using weak passwords that I haven't even mentioned.**

I also realize that most people just don't care about all this until it's too late and they've learned a very hard lesson. But why don't you do me, and yourself, a favor and take a little action to strengthen your passwords and let me know that all the time I spent on this article wasn't completely in vain.

Please, be safe. It's a jungle out there