

# Password Pointers

By Mark D. Spivey, CISSP  
Network Security Engineer

We all have passwords to remember. With passwords for e-mail, network logins, bank accounts, etc... it can become overwhelming and confusing. Unfortunately as human beings we tend to become somewhat complacent with our passwords and not only resist change for fear of forgetting them, but have several other areas of concern.

I have several best practices to help keep you safe. It's imperative to understand that a password is more often than not the weakest link in the chain in regards to security. Don't let your password be the link that breaks.

Security best practices:

- Don't use the same password for each login
- Don't use easy passwords
- Don't use adjoining keys for your password
- Passwords should be 7 or 14+ characters in length
- Passwords should contain Uppercase, lowercase, numbers and special characters
- Don't write down your passwords
- Don't let Windows® remember your passwords
- Don't tell anyone your password
- Change your password frequently
- When in doubt of a compromise, change your password immediately
- Use a phrase instead of a word for a password
- Maintain a current anti-virus solution and operating system updates

Let's look a bit further into each tip:

## **Don't use the same password for each login:**

I'm willing to bet many of you are guilty of this. The problem with using the same password is that this creates a single point of failure. Once your password has been compromised, all your accounts are vulnerable. Use different passwords for each login.

## **Don't use easy passwords:**

How many of you are using passwords consisting of a family name, birth date, pet name, etc? Here's a good rule of thumb: don't use a word in the dictionary.

Many password cracking programs have dictionary lists to help crack the password code.

### **Don't use adjoining keys for your password:**

Many times users will use a keyboard pattern for their password. For example; qwerty or qetuo[ are both pattern passwords – the first one uses six adjoining keys and the second one uses every other key on that row of keys. Again, password cracking programs are familiar with these techniques and contain these patterns in their lists of possibilities.

### **Passwords should be 7 or 14+ characters in length:**

Why 7 or 14+? Windows computers store your password by sending the password you type through a mathematical algorithm that creates what is known as a one-way hash. This value is a representation of your actual password, but not the actual password. The problem is two-fold:

- Windows will actually break your password into seven character blocks before sending it through the algorithm (for backwards compatibility reasons), which means a password of **password1** is actually broken into **passwor** and **d1**. A password cracking program takes very little time to break all the two-character combinations to break the **d1** portion of your password.
- The algorithm used is a known algorithm. This means a password of **password1** always produces the same hash value. Knowing this, the password cracking programs send characters and words through the known algorithm until the resulting hash matches the one stored on your computer. It should be noted that **all** passwords can be broken. It's a matter of making it so difficult to break that the attacker either moves to an easier target, or by the time the password has been broken, it has been changed. The longer the password the better.

### **Passwords should contain uppercase, lowercase, numbers and special characters:**

The most common passwords used are six characters or less, all lower case. It takes no time at all for these passwords to be broken. By using a variety of characters and case, you are making it extremely difficult for your password to be compromised.

A few examples of password comparisons are:

<b>BAD</b>	<b>GOOD</b>	<b>BETTER</b>	<b>BEST</b>
password	PaSsW0rd1	P@sSw0Rd1	w)Rd1\$s@P
fido	F1D0d0G	71D0%oG	%oG^D17
nancydrew	NaNcYDr#w	n@NciEDr3W	W#rdYN@nc

### **Don't write down your passwords:**

How many of you have sticky notes with your passwords on your monitor, under your keyboards, desk calendars, etc? Sticky notes are a password nightmare. When you write passwords down, you are risking the chance of anyone with physical access locating your password, and then the game is over. The idea is to remember your password without having to write it down. One technique to help you do this is to develop a password schema that you can remember.

For example:

- First two letters of my employer's last name (Uppercase/Lowercase/Special Character)
- + Character representation of what the e-mail is used for (**E**mail/**B**ank/**N**etwork)
- + shoe size (6, 7\_5, 12)
- + random word of the week/month (Uppercase/Lowercase/Special Character)

If my random word for the week/month was POLICE, then under this schema my network password would be H#n13p0L1@# (a nice and solid password for a network login).

### **Don't let Windows remember your passwords:**

Even though Windows does a very good job of remembering your passwords, it does a very bad job in keeping them secure. There are many programs freely available on the Internet that can break those passwords instantly. Even though Microsoft® does not promote password security for its "remember your password" feature, Windows does provide you a false sense of security. Don't use it.

### **Don't tell anyone your password:**

This is what I refer to as the “trusted friend” syndrome. Aunt Sally, your brother John, or even your best friend Danny, has no business knowing your password. Here are the basic problems with this condition:

- Someone else may have heard you give them the password.
- Someone else may read the e-mail you sent them containing your password.
- People – even relatives – can get mad at you and conduct activities that threaten your security.
- If you trusted someone else with your password, and they trust “others” as well, your password could be passed around in the “trusted” net of people.
- Chances are – especially at work – you have agreed to keep your password to yourself and not to share it with anyone.

### **Change your password frequently:**

Along with not using the same password for all your logins, changing these multiple passwords frequently is often met with great resistance. Please remember that **all** passwords can be broken – given enough time. The idea behind good passwords is not only to make the passwords resistant to an attack, but if by some chance your password is eventually broken, it has been changed before it can be used.

Many employers require a password change between 30-60 days, but a good rule of thumb is the more frequently you change your passwords the better. Some organizations with highly sensitive data will require passwords to be changed every few hours.

A word of caution in changing your password: don’t fall into the habit of what I have termed an “incremental change.” This occurs when you simply add a number to the end of your password and increment that number by one every time you change your password.

For example;

**Password1** now becomes **Password2**, then **Password3**, etc.

This is a good time to mention one-time passwords. These passwords are only good for one use and are almost impervious to a security breach. Many

companies use security “tokens” that create a random password every 60 seconds or so and are only good for 60 seconds.

**When in doubt of a compromise, change your password immediately:**

If you have **any** concerns that your password may have been compromised, change it immediately. It is best to err on the side of caution with passwords due to the potential damage factor that can be produced from a successful compromise.

Things to watch for that may indicate a password compromise:

- Unknown applications have been installed on your system
- Unknown activity has occurred in your personal bank accounts or other Internet- based areas
- “Jokes” from co-workers containing information concerning your account(s)

**Use a phrase instead of a word for a password**

This is a technique I personally use for all my passwords. I find it much easier to create stronger passwords by using a phrase instead of a single word as my password.

For example:

ILoveJackHenry = 14 characters √ (not strong enough yet)

!L0VeJ@Ck%#nRy = Uppercase/Lowercase/Special Characters √ (very strong)

**Maintain a current anti-virus solution and operating system updates:**

You can invest a million dollars of security in your network and lose everything in an instant because someone doesn't have current anti-virus protection on his computer. A user can easily install a virus or Trojan horse from the Internet and give complete control of the system and/or to an attacker.

I cannot stress enough the importance of maintaining current anti-virus and operating system updates. In 2000, an average of three new viruses or variants of current viruses came out **every day!**

Things to watch out for that may indicate a Virus/Trojan compromise are:

- Unknown applications have been installed on your system.
- Unusual activity occurs on your computer.
  - Hard drive grinding when your not doing any work at the time
  - Mouse moves on its own, Windows/CD tray opens/closes by itself
- Files or folders are missing.

I hope you find these best practices useful not only at work but also at home.

Mark D. Spivey, CISSP  
Network Security Engineer  
Jack Henry & Associates, Inc.  
[mspivey@jackhenry.com](mailto:mspivey@jackhenry.com)