Smarter password management

How to handle your passwords without getting lost

John Locke

Your dog's name… your anniversary… your childrens' initials, birthday, or birth weight… your favorite hobby, or the name of your boat. Which one do you use for your password? Network Administrators and hackers know that most people choose passwords like these to protect anything from logging into web-based bulletin boards to buying things online.

Why does it matter? Identity theft… corporate espionage… loss of your data, or digital images. Do you want to risk these things? In many cases, a weak password is all that separates your data from anyone who wants to impersonate you online, or worse.

The problem with weak passwords

Passwords that are simply names of pets, names of children, common names of any type, are called "weak passwords." Basically any word you can find in a dictionary or list of names makes for a weak password.

I don't like to use fear to motivate people, but practicing safe password management is as important as locking your house when you leave. Only whenever you're connected to the internet, it's like having a house in the worst neighborhood in the biggest city around and if you don't put a good lock on the door, you will get broken into, even if you're home.

The problem with strong passwords

If you work at a large company, they may not allow you to have a simple password based on any word you can find in a dictionary. E-Commerce sites that have good security require passwords at least 8 characters long. They group the characters you type into four groups: capital letters, lowercase letters, numbers, and symbols, and then require you to have at least three out of the four groups represented in your password. And then they make you change your password every two or three months. This type of password is called a strong password.

Practicing safe password management is as important as locking your house when you leave

The problem is that you soon end up with many more passwords than you can possibly keep track of. You either forget your new password, requiring the administrator to reset it for you, or you start writing them down. Far too many people have their current passwords scribbled on a yellow sticky note attached to their monitor where anyone can see it.

With weak passwords, all an attacker needs to do to obtain them is go through your trash, or engage you in innocent conversation. With strong passwords, all he needs to do is visit your office. In either case, the attacker is engaging in a type of attack called *Social Engineering*, which is the easiest way to break into a system.

Do I always need a strong password?

No. Strong passwords provide far more protection against different types of attacks, especially those considered *Brute*

Force attacks. An example is something called a *Dictionary Attack*, where the attacker takes a list of words, sometimes an entire dictionary, and uses a special cracking program to try each word on your account. The dictionary used includes common animal and people names.

Many systems defeat these types of attacks by locking you out after a few failed attempts. But the real concern is what an attacker can do once they break into any particular system.

Assess your risks

There are low risk, and high risk computer systems. To avoid having 30 different passwords to remember, you can group together systems that have the same level of risk, and reuse your passwords. Many security experts would argue that this approach reduces security, but let's be realistic here: if you don't remember the password for a particular system, and then type in all of your "standard" passwords to try to log into it, you may have just compromised all of the systems that use any of those passwords.

There are many ways of grouping systems, but here's what I recommend:

Low risk systems

If you never give your credit card, drivers license, social security number, or any other sensitive information to a web site, you probably don't need to use a strong password. For sites like the New York Times, online bulletin boards, and the myriad of places that ask you to create an account before allowing you to post, use a throw-away, easy-to-remember password. The worst an attacker could do is impersonate you on a web site, a mild form of harassment, but nothing more serious than that.

You should realize that any time you type a password into a system that doesn't immediately take you to an encrypted site, your password could be intercepted by all kinds of unknown people. Look for the lock or key icon in your browser's status bar, and "https" in the web address. If these things don't appear, or there's a warning, don't trust the site. Use a weak password, and consider it public. As long as you trust a site as being legitimate, I consider it fine to reuse the same weak password for all of these types of sites.

Medium risk systems

You might not agree, but I consider credit card information to be medium risk. To purchase things using a credit card at all, you have to take some risk: the waiter at the restaurant could copy your card when taking your payment; somebody could eavesdrop on your cordless phone when you give the number to the pizza delivery place; or somebody could look over your shoulder in line at a store.

Credit Card companies provide you with protection here - you're usually only liable for the first $50 of any misuse of your credit card. For many credit cards, the bank takes full risk for online payments. You have to report charges you did not make in writing within 60 days, and these guarantees don't apply to debit cards, but overall loss of your credit card amounts to a bigger hassle but not devastation to your identity. So I recommend grouping all web sites you use a credit card for into a "medium risk" group. If you give a web site a credit card, you're already trusting them to not make bogus charges so you can probably trust them to not try to use your strong password on other sites.

> A weak password is all that separates your data from anyone who wants to impersonate you online, or worse

Some cautions here:

- Never send a credit card number, or any more sensitive information, through an email system that is not encrypted. If your email system is encrypted, you'll know it: you'll have to do quite a bit of work on both the sending and receiving end, so assume your mail is completely insecure, because it is.
- Always make sure the web site is encrypted before typing in your password. Look for the lock or key icon in your browser window. In Firefox, the address bar (where you type the web address) will turn yellow if it's properly encrypted.
- Never use a public computer to make web transactions. Even if the web site is encrypted, there could be snooping software installed on the computer that could get your user account and password as you type it. Only conduct sensitive transactions on computers you trust and get the spyware off first!
- Just because a web site is encrypted, doesn't mean your data is protected. Many smaller companies have not invested in proper security to protect your password and credit card information. If in doubt, look for a security statement, or ask! If your business would like to properly secure customer data, contact Freelock Computing (`http://freelock.com/mail.php`) and let's talk!

High risk systems

Any system that contains your social security number, drivers license number, or other financial account numbers should be considered high risk. Systems that contain sensitive business information should be protected with a strong password, and if they're connected to the internet, that password should be changed frequently.

As a general rule, never give your password to anyone, especially not a password you use in other medium or high-risk systems

For the most part, this means treating your laptop or workstation as a high-risk system so use a different password to log into it than you use for e-commerce or general use.

In most cases, you can get by with three passwords, using them on the appropriate level of system: a weak password for general, low risk systems; a strong password for e-commerce and medium risk systems, and a different strong password for any computer you use that has business or sensitive information on it. In some cases, this isn't enough. If you have critical systems that contain personally identifiable customer data, or administrative access on customer machines, you may need to manage dozens of passwords. We'll cover how to securely manage dozens of passwords, as well as create strong ones, next month.

As a general rule, never give your password to anyone, especially not a password you use in other medium or high-risk systems. If you're getting help from somebody who administers a service for you, they will be able to set your password to something else without knowing your password.

Copyright information

About the author

John Locke is the author of the book *Open Source Solutions for Small Business Problems.* He provides technology strategy and open source implementations for small and growing businesses in the Pacific Northwest through his business, Freelock LLC (`http://www.freelock.com`).