Password Management Ideas

Or

IS Password Management Important?

Joel Peter Anderson
University Information Security
Here are some of the reasons why having a good password — AND GOOD PASSWORD MANAGEMENT(!) matters.
IS Password Management Important?

AP’s Twitter Feed Hacked — Stocks Briefly Plunge

... that would be a yes, I think....
IS Password Management Important?

Onion's Twitter account hacked by Syrian Electronic Army

Apparently, the tweets sympathetic to Syrian President Bashar Assad aren't a laughing matter -- the parody news site's feed is the latest to be vandalized in ongoing attacks against news outlets.

C'mon it's hard to deal with passwords....

...but there are solutions....
Onion IT specialist Nick Abersold, who noted that the new password’s length and use of numbers makes it “virtually impenetrable.” “There are no spaces, and the O and M are both capitalized—both tactics that I think will keep us safe for the foreseeable future. Also, there’s not one, but two 7s. So, once again, The Onion’s Twitter password is OnionMan77.” Abersold added that in order to ensure continued electronic security throughout The Onion’s operations, he had also reset the password for its Facebook page, employee email accounts, and mainframe server to OnionMan77. ….

Um – that might not be a good answer....
Passwords are tricky – but maybe not
As tricky as we sometimes think.....
In *Password Memorability and Security: Empirical Results* the authors did an experiment that tested password creation, strength and retention with three groups of students.

1. Naïve password choices (control)
2. Totally random choice
3. “Mnemonic phrase” password

(they also compared their subjects to a random sample of student accounts.)

*This study* confirmed

• users have difficulty remembering random passwords

• passwords based on mnemonic phrases are harder to guess than naïvely selected passwords.

debunked

• random passwords are better than passwords based on mnemonic phrases. In fact, each appeared to be as strong as the other.

• passwords based on mnemonic phrases are harder to remember than naively selected passwords. In fact, each type is as easy to remember as the other.
So... how do I come up with a good password?
From SANS OUCH May 2013:

The best way to create a strong password is to use a long password, and the more characters you have, the better. In fact, instead of using a single word, use multiple words -- or even a complete sentence. This type of password is called a passphrase, and it is one of the strongest you can use. Here is an example of one:

**time for my coffee**

That is it; that is all you need. If required, you can make your password even stronger by adding symbols, capital letters or numbers, such as those you see in the example below. This is especially important if you are using a website that does not allow multiple words or a complete sentence for your password:

**Time f0r my coffee!**

Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.

XKCD got it right...
I FORGOT MY p4sSWo0Rd AGAIN.
Go with easy to remember, hard to hack.
It’s about length, not complexity.

FROM: “Br3ak1ead&7”
HACK: 28 Bits of Entropy | 2^{28} Combinations
CRACK: 3 Days at 1000 guesses/sec

TO: “thunder showers before sunset”
HACK: 44 Bits of Entropy | 2^{44} Combinations
CRACK: 550 Years at 1000 guesses/sec

... hm those are the same numbers....
A Password PLUS Strategy

Some recommend developing a system where you choose a complex password to which you ADD a suffix or prefix to tie it to specific services. For example start with a phrase from Much Ado About Nothing:

- These gloves the Count sent me + tweet
- These gloves the Count sent me + gml
- These gloves the Count sent me + hotmail

Gives you a chance to memorize Shakespeare AND have a complex and hard-to-crack password.
Google 2-Step Verification

Stronger security for your Google Account

With 2-Step Verification, you'll protect your account with both your password and your phone

Why you need it  How it works  How it protects you

http://www.google.com/landing/2step/

Note: if you can, 2 factor authentication is great!
... there are some good tips here, too:

While you're at it, you can test your password.... er, you can try things LIKE your password to see how they measure up.

(please DON'T use your real, live password in testing websites.....)
Check your password - is it strong?

Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them.

**Test the strength of your passwords:** Type a password into the box.

Password: 

Strength: 

**Note:** This does not guarantee the security of the password. This is for your personal reference only.

**What is a strong password?**

The strength of a password depends on the different types of characters that you use, the overall length of the password, and whether the password can be found in a dictionary. It should be 8 or more characters long.

For tips about how to create passwords that are easy for you to remember but difficult for others to guess, read [Create strong passwords](https://www.microsoft.com/security/pc-security/password-checker.aspx).

**About this password strength checker**

Microsoft does not retain information entered into this password checker. The password you enter is checked and validated on your computer. It is not sent over the internet.

HOW SECURE IS MY PASSWORD?

Enter Password

This site could be stealing your password... it's not, but it easily could be.
Be careful where you type your password.

http://howsecureismypassword.net/
### How Secure is My Password?

- **Your password would be cracked almost instantly.**

### Common Password: In the Top 2330 Most Used Passwords

- **Possibly a Word**
  - Your password looks like it could be a dictionary word or a name. If it’s a name with personal significance it might be easy to guess. If it’s a dictionary word it could be cracked very quickly.

- **Character Variety: Just Letters**
  - Your password only contains letters. Adding numbers and symbols can make your password more secure.

- **Length: Short**
  - Your password is quite short. The longer a password is the more secure it will be.

---

Oops, maybe I'm not the only SF fan.....
How secure is my password?

It would take a desktop PC about
49 million years
to crack your password

[Tweet Result]
Think of your password like groceries:

**You don't want junk**
- follow good advice for a unique, complex, password

**You want to keep them fresh**
- as soon as you start using a password, the chance it will be discovered slowly increases. Every time you replace it, you reassert your control and ownership.

*It's to your advantage to replace your password on a regular basis*

**Keep them safe**
- you keep your food in the freezer or the fridge; use “best practice” tools to manage and store your passwords.
With one IMPORTANT exception:

**PLEASE**
**DO NOT**
**SHARE!**

Once anyone other than you knows your password, it really isn't *your* password. No one other than you should know your password.
ONCE you have the password, now what?

- Memorize it!
  http://en.wikipedia.org/wiki/Mnemonic

- Write it down!
  http://www.schneier.com/blog/archives/2005/06/write_down_your.html

- Use a tool!
Wait! **Write it down?!?**

Carry your passwords on paper, in your pocket. This is a somewhat controversial solution promoted by security expert Bruce Schneier — even though he wrote the digital password management program Password Safe. Schneier advocates that people keep their passwords in their wallets. What you sacrifice in security, the argument goes, is made up for by the convenience — with easy access to your passwords, you’re more likely to use very strong ones that you couldn't remember otherwise, plus you can access your passwords even when you're away from your computer. An added benefit is that when your passwords are in your wallet, you'll find out very quickly if they've been lost or stolen.

However, to mitigate the risk of a loss, add a certain number of dummy characters before and after the real passwords to make it harder to identify them, and use simple code-words to indicate what asset they protect, rather than saying "Chase Manhattan Bank" or "Work Computer."

https://ssd.eff.org/your-computer/protect/passwords
Tool tips

what should you look for in a password keeper?

- Based on strong cryptography
  Does it securely store your information?

- Open Source
  Benefit from active development community; no secrets, no snake oil

- Portable
  Can you use it easily on more than one computer? Can it run from a flash drive?
Some good assessment and links to a good set of tools:

1. Keepass
2. 1Password
3. LastPass
4. RoboForm
5. Password Safe

http://www.freepasswordmanager.com/
Locknote

https://www.steganos.com/us/products/for-free/locknote/overview/
http://sourceforge.net/projects/locknote/
A very simple Windows program – it's *notepad*... with AES Crypto.
Even works in Ubuntu under Wine!
References:

**Password Memorability and Security: Empirical Results**

**Learn How to Use Passwords Properly**
https://ssd.eff.org/your-computer/protect/passwords

**See also the EFF’s Surveillance Self-Defense Project**
https://ssd.eff.org/

**SANS OUCH:** http://www.securigthehuman.org/newsletters/ouch/issues/OUCH-201305_en.pdf


**Google 2-Factor:** http://www.google.com/landing/2step/

**Password Strength Tests:**
- http://howsecureismypassword.net/

**Tools:**
http://www.freepasswordmanager.com/
https://www.steganos.com/us/products/for-free/locknote/overview/
http://sourceforge.net/projects/locknote/