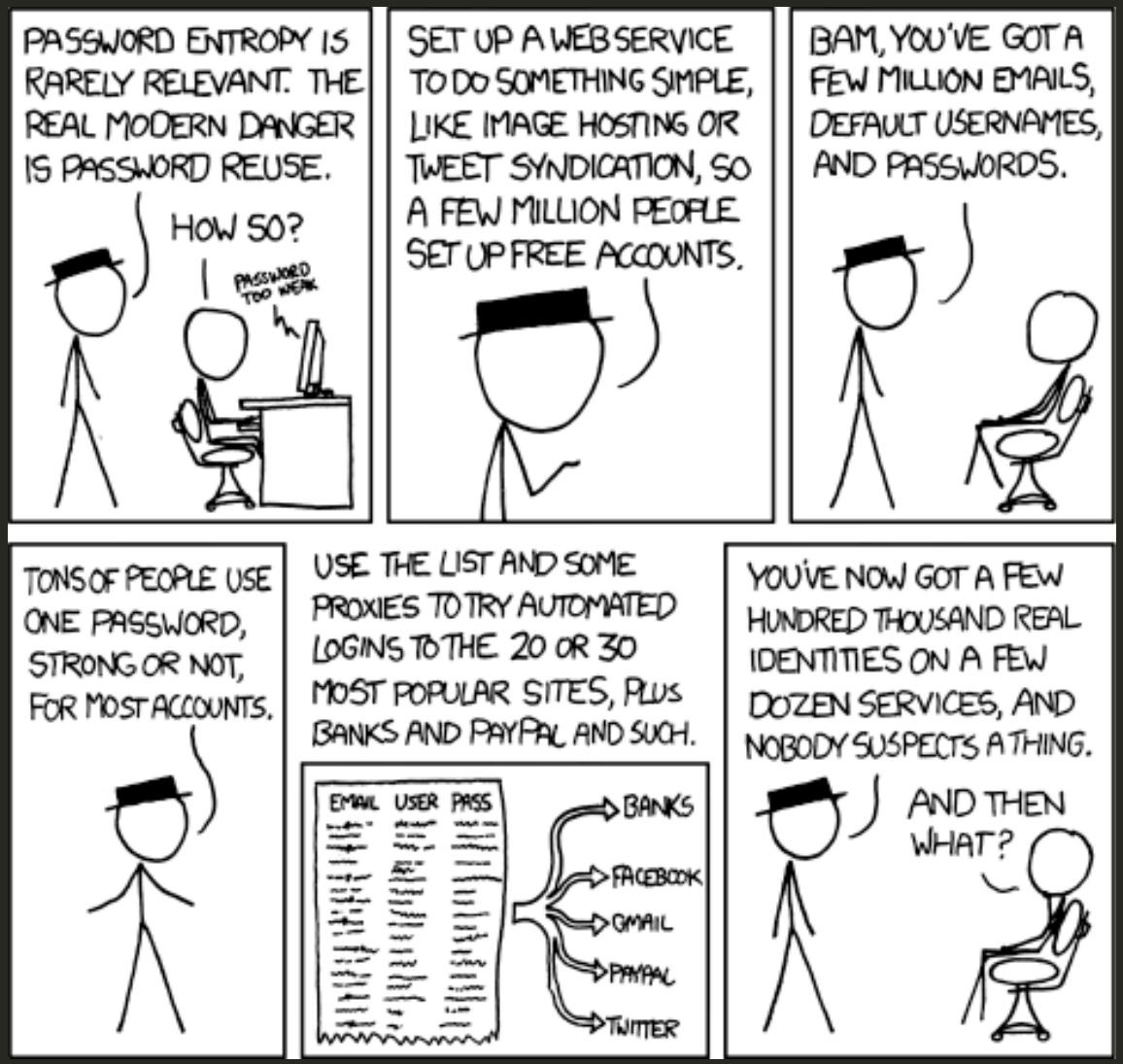
Surviving phishing

Password reuse, password managers and strong passwords

Contents

Why is Password Reuse a Problem?



Consider the following hypothetical users that reuse a strong password in most places and the following common scenario:

User	Password
mark1@gmail.com	QUo5Qt+1Wa/Q1smDJRDbFg==
mark2@gmail.com	+9Hz+/20rVkSkbcsmgdVFw==
mark3@gmail.com	wnYkRcbi7Kkh7Fx2uR8EeA==

1. User registers an account with a careless service, eg Facebook, Yahoo, Google, Equifax etc. etc.
2. The service is hacked and the password and email is leaked
3. The hacker logs in to the email account
4. The hacker resets passwords on all important accounts tied to that email address

About password strength

How is strength measured?

'Entropy' *s* depends on the size of the alphabet *a* and the length *n* of the password:

$$s = log_2(a^n)$$

- 0889234877724602 -> 53 bits
- ZeZJieatdH -> 60 bits

Why are weak passwords problematic?

Weak passwords are trivial to crack in many situations. A password with 53 bits may be cracked by a criminal organisation in less than an hour.

What about strong passwords?

They are difficult to remember, a problem especially when you use a different strong password for every service. You are also tempted to write them down, or reuse them.

It's surprisingly difficult for humans to generate good passwords!

A strong password, as of 2019, has at least 80 bits of entropy.

Password Managers to the Rescue!

Password managers allow you to create a unique and strong password for every service.

Additional benefits:

- Remembers passwords for you
- Generates passwords for you
- Automagically fills in passwords on websites for you, this is important!
- Makes passwords available on all your configured devices
- Can store additional related data, usernames, answers to security questions, pins for debit/credit cards

Any of the mainstream password manager is equivalent in the above respects.

Can you trust password managers?

Yes*

How do they keep passwords secure?

1. User supplies a password
2. A slow function derives an encryption key
3. The encryption key is used to encrypt/decrypt your passwords

Security of the encryption depends on the strengh of your password:

Entropy	Time to crack, assuming 1 second per attempt per typical CPU
50b	< 1 Month
60b	~ 50 Years
70b	~ 50,000 yers

Generating a Strong Password

Passphrases are better than passwords:

- Tr0ub4dor&3 -> 28 bits of entropy, hard to remember
- correct horse battery stable -> 44 bits of entropy, easy to remember

If you have to remember it, use a passphrase.

Generate passphrases with Diceware [1]

1. Roll 5, 6 sided, *physical* dice
2. Read the numbers left to right
3. Find the word with that number on a list 6^5 (7776) words
4. Repeat until desired length is reached. For a password manager, use at least 7.

5. Write down your passphrase on paper and keep it somewhere secure
6. If you are 100% confident that you will not forget the passphrase, destroy the paper by burning

What about phishing?

- A password manager will refuse to fill out a password on a spoofed website, for instance faceb00k.com vs facebook.com
- Using different passwords on every service protects all other services even if phishing is successful on one of them
- Good password managers will navigate to the login page for you, reducing the risk of spoofed websites

Other advice

In no particular order:

- Only log in on webpages that you navigated to by typing in the url yourself, by searching on google, duckduckgo or some other reputable search engine or from a bookmark. If after clicking a link in an email you are directed to a log in page, it's probably a phishing attempt
- Only log in to webpages that are protected by SSL/TLS (HTTPS). Look for a green address bar, or a green lock icon or similar in your browser
- Use two factor or two step authentication everywhere if possible
- Turn of automatic image rendering. Better still, disable HTML rendering and authoring entirely in your email client
- Be suspicious of *all* emails. Risky things: HTML email, images, unknown sender, poor spelling/grammer, 'Your email client can't display this email, click here to view in your browser' or similar attempts to coerce you to click on things

Resources

EFF notes on Diceware [2] They generally have good advice for these kinds of topics.

This Presentation [3]

Keepass [4], an offline password manager

1Password [5], a pay to use password manager with some nice features

LastPass [6], an online password manager with a gratis tier

1 http://world.std.com/~reinhold/diceware.html
2 https://www.eff.org/dice
3 https://git.friedersdorff.com/max/intro_dice_and_pmgmnt
4 https://keepass.info/
5 https://1password.com/
6 https://www.lastpass.com/